Kaspersky Anti-Virus 8.0 für Microsoft ISA Server und Forefront TMG Standard Edition

ADMINISTRATORHANDBUCH

PROGRAMMVERSION: 8.0

Sehr geehrter Benutzer!

Wir danken Ihnen, dass Sie unser Programm ausgewählt haben. Wir hoffen, dass Ihnen diese Dokumentation hilft und die meisten Fragen damit beantwortet werden können.

Achtung! Die Rechte an diesem Dokument sind Eigentum von Kaspersky Lab ZAO (im Folgenden auch Kaspersky Lab) und durch die geltenden Gesetze der Russischen Föderation zum Schutz von Urheberrechten sowie durch internationale Verträge geschützt. Bei illegalem Kopieren und Weiterverbreiten des Dokumentes und seiner einzelnen Teile haftet der Zuwiderhandelnde nach dem Zivilrecht, Verwaltungsrecht oder Strafrecht der Russischen Föderation.

Das Kopieren in jeder Form, wie auch das Weiterverbreiten durch Übersetzungen, von Unterlagen ist nur mit einer schriftlichen Einwilligung von Kaspersky Lab erlaubt.

Das Dokument und die damit verbundenen grafischen Darstellungen dürfen nur zu informativen, nicht gewerblichen oder persönlichen Zwecken gebraucht werden.

Das Dokument kann ohne vorherige Ankündigung geändert werden. Die neueste Version des Dokumentes finden Sie auf der Seite von Kaspersky Lab unter http://www.kaspersky.com/de/docs.

Für den Inhalt, die Qualität, die Richtigkeit und Vertrauenswürdigkeit der im Dokument verwendeten Unterlagen, deren Rechte anderen Rechteinhabern gehören, sowie für Schäden, die in Verbindung mit der Nutzung dieser Unterlagen entstehen, lehnt Kaspersky Lab die Haftung ab.

In diesem Dokument werden eingetragene Markenzeichen und Handelsmarken verwendet, die das Eigentum der jeweiligen Rechteinhaber sind.

Redaktionsdatum: 13.10.2010

© 1997-2010 Kaspersky Lab ZAO. Alle Rechte vorbehalten.

http://www.kaspersky.com/de
http://support.kaspersky.com/de/

INHALT

LIEFERUMFANG 6
Lizenzvertrag 6
Service für registrierte Benutzer 6
KASPERSKY ANTI-VIRUS 8.0 FÜR MICROSOFT ISA SERVER UND FOREFRONT TMG STANDARD EDITION 7
Wesentliche Programmfunktionen 7
Hard- und Softwarevoraussetzungen 7
PROGRAMMARCHITEKTUR 10
SCHUTZ FÜR CLIENT-COMPUTER INSTALLIEREN 12
PROGRAMM INSTALLIEREN 13
Programminstallation vorbereiten 13
Aktualisierung von Vorgängerversionen 13
Vorgehen bei der Installation 13
Schritt 1. Überprüfen des Systems bezüglich der Installationsvoraussetzungen 14
Schritt 2. Begrüßungsfenster des Installationsassistenten 14
Schritt 3. Lesen des Lizenzvertrags 14
Schritt 4. Installationstyp auswählen 15
Schritt 5. Benutzerdefinierte Installation 15
Schritt 6. Datenspeicherordner auswählen 16
Schritt 7. Regel für Remoteverwaltung anpassen 17
Schritt 8. Dateien kopieren und Programmkomponenten registrieren 17
Schritt 9. Installationsvorgang abschließen 17
Programm aktivieren. Verschiedene Methoden zur Aktivierung des Programms 18
Änderungen am System nach Installation des Programms 18
Vorbereitung zur Verwendung des Programms 19
Programm wiederherstellen 19
Programm deinstallieren 20
Abschlusseinrichtungsassistent 20
LIZENZVERWALTUNG 22
Programm aktivieren 22
Reserveschlüssel hinzufügen 23
Benachrichtigung zum Ablauf der Lizenz anpassen 24
PROGRAMMOBERFLÄCHE 25
Programmhauptfenster 25
Programmeinrichtungsfenster 26
PROGRAMM STARTEN UND BEENDEN 28
MANAGEMENT-KONSOLE MIT DEM SERVER VERBINDEN 29
ÜBERPRÜFUNG DER PROGRAMMEINSTELLUNGEN 30
Schutz für Datenströme über das HTTP-Protokoll überprüfen 31
Schutz für Datenströme über das FTP-Protokoll überprüfen 31
Schutz für Datenströme über das SMTP / POP3-Protokoll überprüfen 31

GRUNDEINSTELLUNGEN FÜR DEN DATENSTROM-SCHUTZ....32
DATENBANKUPDATES....33
Statusinformationen zu Datenbanken abrufen....33
Manuelles Update der Datenbanken....34
Automatisches Update der Datenbanken....34
Updatequelle für Datenbanken auswählen....35
Einstellungen für Datenbankupdates über Internet anpassen....36
Datenbankupdate aus einem Netzwerkordner....37
Update aus einem Netzwerkordner: Kaspersky Anti-Virus innerhalb einer Domain....37
Update aus einem Netzwerkordner: Kaspersky Anti-Virus innerhalb einer Arbeitsgruppe....38
VIRENPRÜFUNG....39
Performanceeinstellungen für die Virenprüfung anpassen....39
Einstellungen für die Überwachung des Datenstroms über das HTTP-Protokoll anpassen....40
Einstellungen für die Überwachung des E-Mail-Verkehrs über FTP-Bericht anpassen....41
Einstellungen für die Überwachung des Datenstroms über SMTP-Protokoll anpassen....42
Einstellungen für die Überwachung des Datenstroms über POP3-Protokoll anpassen....43
RICHTLINIEN FÜR DIE VIRENPRÜFUNG PFLEGEN....44
Richtlinien für die Verarbeitung von Protokollen....45
Richtlinien für Ausnahmen von der Prüfung....46
Richtlinien für die Virenprüfung....46
Regeln zu Richtlinien hinzufügen....46
Priorität für Regeln in Richtlinien ändern....49
Einstellungen für Regeln in Richtlinien ändern....49
Regeln in Richtlinien deaktivieren....49
Regeln in Richtlinien löschen....50
NETZWERKOBJEKTE....51
Netzwerkobjekte erstellen....51
Einstellungen für Netzwerkobjekte ändern....53
Netzwerkobjekte löschen....53
BERICHTE....54
Tasks zur Berichtserstellung erstellen....55
Berichte anzeigen....55
Berichte löschen....56
Tasks für Berichtserstellung löschen....56
Eigenschaften für die Berichtserstellung ändern....56
Allgemeine Eigenschaften von Berichten ändern....56
Statistikdaten für Berichte löschen....57
MONITORING DER PROGRAMMAUSFÜHRUNG....58
Ausführungsstatus von Kaspersky Anti-Virus....59
Statistik zur Ausführung von Kaspersky Anti-Virus....60
BACKUP-ORDNER....61
Funktionseinstellungen für den Backup-Ordner....62
Informationen zu Objekten im Backup-Ordner anzeigen....62
Ansicht des Backup-Ordners anpassen....63
Objektliste dynamisch filtern....63
Statischen Filter für Backup-Ordner erstellen....64

Objekte aus dem Backup-Ordner auf Datenträgern speichern 64
Objektliste des Backup-Ordners speichern 64
Objekte aus dem Backup-Ordner löschen 65
DIAGNOSE 66
SPEICHERORT FÜR DEN DATENSPEICHERORDNER DES PROGRAMMS ÄNDERN 68
ÜBERWACHUNG FÜR DATENSTRÖME ÜBER DAS HTTPS-PROTOKOLL AKTIVIEREN 69
ANHANG 1. ÄNDERUNGEN IN DER MICROSOFT WINDOWS REGISTRY 70
INFORMATIONEN ZUM CODE VON DRITTHERSTELLERN 73
Programmcode 73
A C# IP ADDRESS CONTROL 73
BOOST 1.36.0, 1.39.0 74
EXPAT 1.2 74
LOKI 0.1.3 74
LZMALIB 4.43 75
MICROSOFT CABINET SOFTWARE DEVELOPMENT KIT 75
SQLITE 3.6.18 75
WIX 3.0 75
ZLIB 1.0.8, 1.2, 1.2.3 78
Sonstige Informationen 78
ENDNUTZER-LIZENZVERTRAG FÜR KASPERSKY LAB SOFTWARE 79
TERMINOLOGISCHES GLOSSAR 85
KASPERSKY LAB 89
SACHREGISTER 90

LIEFERUMFANG

Kaspersky Anti-Virus 8.0 für Microsoft ISA Server und Forefront TMG Standard Edition (im Folgenden auch Kaspersky Lab) kann bei unseren Vertriebspartnern oder in einem Online-Shop (z.B. http://www.kaspersky.com/de, Abschnitt E-Store) erworben werden. Kaspersky Anti-Virus ist Teil von Kaspersky Total Space Security (http://www.kaspersky.de/total_space_security) und Kaspersky Security für Internet Gateway (http://www.kaspersky.de/kaspersky_security_internet_gateway). Nach dem Erwerb einer Lizenz für Kaspersky Anti-Virus erhalten Sie per E-Mail einen Link für den Download des Programms und des Aktivierungsschlüssels von unserer Homepage

IN DIESEM ABSCHNITT

Lizenzvertrag 6

Service für registrierte Benutzer 6

LIZENZVERTRAG

Der Lizenzvertrag ist ein juristischer Vertrag zwischen Ihnen und Kaspersky Lab, in dem steht, unter welchen Bedingungen Sie das von Ihnen gekaufte Programm gebrauchen dürfen.

Lesen Sie sich die Lizenzvereinbarung genau durch!

Möchten Sie den Lizenzvertrag nicht akzeptieren und das Programm nicht nutzen, haben Sie Anspruch auf Erstattung des Kaufpreises.

SERVICE FÜR REGISTRIERTE BENUTZER

Kaspersky Lab bietet den legalen Benutzern ein umfangreiches Spektrum an Leistungen an, die den wirkungsvollen Einsatz des Programms effektiver gestalten.

Wenn Sie eine Lizenz erwerben, werden Sie ein registrierter Benutzer und können während der Gültigkeitsdauer der Lizenz folgende Leistungen in Anspruch nehmen:

- Stündliches Update der Programm-Datenbanken und Angebote neuer Versionen für dieses Programm;
- Konsultation zu Fragen bei der Installation, Konfiguration und zum Betrieb der Software; Telefon und E-Mail;
- Benachrichtigung bei Erscheinen von neuen Kaspersky-Lab-Programmen und bei neu aufgetauchten Viren. Diese Leistung wird Benutzern geboten, die den Newsletter von Kaspersky Lab auf der Webseite des Technischen Supports (http://support.kaspersky.com/de/subscribe/) abonniert haben.

Es werden allerdings keine Fragen zu Funktion und Gebrauch von Betriebssystemen, zu Programmen von Dritten sowie zu verschiedenen Technologien beantwortet.

KASPERSKY ANTI-VIRUS 8.0 FÜR MICROSOFT ISA SERVER UND FOREFRONT TMG STANDARD EDITION

Kaspersky Anti-Virus 8.0 für Microsoft ISA Server und Forefront TMG Standard Edition garantiert für alle Mitarbeiter Ihres Unternehmens sicheres Arbeiten, indem über HTTP-, FTP-, SMTP- und POP3-Datenströme empfangene schädliche und potenziell gefährliche Objekte automatisch gesperrt werden.

In diesem Abschnitt

Wesentliche Programmfunktionen 7

Hard- und Softwarevoraussetzungen 7

Wesentliche Programmfunktionen

Kaspersky Anti-Virus bietet Ihnen:

- Überwachung des HTTP-, FTP-, SMTP- und POP3-Datenstroms in Echtzeit.
- Überwachung des eingehenden Datenstroms über HTTPS (nur für Forefront TMG).
- Große Auswahl an Filterkriterien für den Datenstrom durch Verwendung von Gruppen von Netzwerkobjekten und Überwachungsregeln.
- Stets aktueller Schutzstatus durch laufende Updates der Antiviren-Datenbanken.
- Aufspüren potenziell gefährlicher Programme.
- Überwachung der Ausführung von Kaspersky Anti-Virus in Echtzeit
- Vollständige Informationen zur Ausführung von Kaspersky Anti-Virus durch benutzerdefinierte Berichte.
- Aufbewahrung von Kopien gesperrter Objekte in einem geschützten Backup-Ordner.
- Individuell angepasste Performanceeinstellungen für die Virenprüfung in Abhängigkeit von Serverkapazität und Übertragungsgeschwindigkeit der Internetverbindung.
- Dynamische Auslastung der Serverprozessoren.
- Remoteverwaltung für Kaspersky Anti-Virus über die als Standard-Toolkonsole ausgelegte Management-Konsole.

Hard- und Softwarevoraussetzungen

Softwarevoraussetzungen für Computer zur Installation von Kaspersky Anti-Virus:

1. Eines der folgenden Betriebssysteme:
    - Zur Verwendung von Kaspersky Anti-Virus mit Microsoft ISA Server 2006 Standard Edition:

- Microsoft Windows Server 2003 SP2.
- Microsoft Windows Server 2003 R2.

- Zur Verwendung von Kaspersky Anti-Virus mit Forefront TMG Standard Edition:
  - Microsoft Windows Server x64 2008 SP2.
  - Microsoft Windows Server x64 2008 R2.

2. Microsoft Management Console 3.0.
3. Microsoft .NET Framework 3.5 SP1.
4. Microsoft ISA Server 2006 Standard Edition/ Forefront TMG Standard Edition Console.

Um Kaspersky Anti-Virus mit Microsoft ISA Server 2006 Enterprise Edition oder Forefront TMG Enterprise Edition gemeinsam zu verwenden, müssen folgende Voraussetzungen erfüllt sein:

- Im Firmennetzwerk darf nur ein Massiv vorhanden sein;
- Im Massiv darf nur ein Server vorhanden sein;
- das Installationsverzeichnis muss sich auf demselben Server befinden, wie Kaspersky Anti-Virus.

Bei Verbindung eines isolierten Servers Forefront TMG Enterprise Edition mit einem autonomen (standalone) bzw. einem Unternehmens-Array (EMS-managed) wird Kaspersky Anti-Virus funktionsunfähig. Die Deinstallation von Kaspersky Anti-Virus mit Standardmitteln des Betriebssystems ist in diesem Fall auch nicht möglich. Durch das Löschen des Servers aus dem Array kann Kaspersky Anti-Virus weder wiederhergestellt noch richtig deinstalliert werden.

Dieses Funktionsschema wird durch die technischen Besonderheiten von Forefront TMG Enterprise Edition verursacht.

Hardwarevoraussetzungen für Computer zur Installation von Kaspersky Anti-Virus:

1. Zur Verwendung von Kaspersky Anti-Virus mit Microsoft ISA Server 2006 Standard Edition:
   - Prozessor 1 GHz;
   - 1 GB Arbeitsspeicher.
   - 2.5 GB freier Festplattenspeicher.
2. Zur Verwendung von Kaspersky Anti-Virus mit Forefront TMG Standard Edition:
   - 64-Bit-Prozessor mit 2 Kerneln;
   - 2 GB Arbeitsspeicher.
   - 2.5 GB freier Festplattenspeicher.

Softwarevoraussetzungen für Computer zur Installation der Management-Konsole:

1. Eines der folgenden Betriebssysteme:
   - Microsoft Windows 7 x64 Professional / Enterprise / Ultimate Edition;
   - Microsoft Windows 7 Professional / Enterprise / Ultimate Edition;
   - Microsoft Windows Server 2008 x64 Enterprise / Standard Edition;

- Microsoft Windows Server 2008;
- Microsoft Windows Server 2003 x64 R2 Enterprise / Standard Edition;
- Microsoft Windows Server 2003 x64 Enterprise / Standard Edition;
- Microsoft Windows Server 2003 x64 SP2;
- Microsoft Windows Server 2003 SP2;
- Microsoft Windows Vista x64;
- Microsoft Windows Vista.

2. Microsoft Management Console 3.0.
3. Microsoft .NET Framework 3.5 SP1.
4. Microsoft ISA Server 2006 Standard Edition/ Forefront TMG Standard Edition Console.

Hardwarevoraussetzungen für Computer zur Installation der Management-Konsole:

- Prozessor 1 GHz;
- 1 GB Arbeitsspeicher.

PROGRAMMARCHITEKTUR

Kaspersky Anti-Virus wird auf Server vom Typ Microsoft ISA Server / Forefront TMG installiert und schützt die angeschlossenen Client-Computer vor schädlichen Objekten, indem der über Microsoft ISA Server / Forefront TMG fließende HTTP-, FTP-, SMTP- und POP3 Datenstrom abgefangen wird.

Für Forefront TMG wird auch der über das HTTPS-Protokoll eingehende Datenstrom überwacht. Für die Überwachung des Datenstroms über das HTTPS-Protokoll müssen Sie keine besonderen zusätzlichen Einstellungen vornehmen. Es werden die für das HTTP-Protokoll gewählten Einstellungen verwendet. Für die Überwachung des Datenstroms per HTTPS-Bericht durch Kaspersky Anti-Virus müssen Sie die Überwachung des Datenstroms in der Management-Konsole von Forefront TMG aktivieren (s. Abschnitt "E-Mail-Überwachung für HTTPS-Bericht aktivieren" ab S. 69).

Kaspersky Anti-Virus umfasst folgende Programmkomponenten:

- **Anti-Viren-Filter** – diese Komponente wird während der Programminstallation in Microsoft ISA Server / Forefront TMG integriert. Es gibt folgende Filtertypen:

  - Web – übernimmt das Abfangen des eingehenden E-Mail-Verkehrs über das HTTP-Protokoll;
  - FTP – übernimmt das Abfangen des eingehenden E-Mail-Verkehrs über das FTP-Protokoll;
  - SMTP – übernimmt das Abfangen des eingehenden und ausgehenden E-Mail-Verkehrs über das SMTP-Protokoll;
  - POP3 – übernimmt das Abfangen des eingehenden und ausgehenden E-Mail-Verkehrs über das POP3-Protokoll.

  Die Filter fangen den Datenstrom über die entsprechenden Protokolle ab, laden die von den Client-Computern angefragten Objekte herunter und übertragen die vollständig geladenen Objekte an das Subsystem für die E-Mail-Prüfung. Nach der Virenprüfung übertragen die Filter die angefragten Objekte an die betreffenden Client-Computer oder informieren den Benutzer durch eine entsprechende Meldung, dass die betreffenden Objekte gesperrt wurden.

- **Subsystem für die Virenprüfung**: Programmkomponente, durch die Objekte auf vorhandene Viren untersucht werden. Von Kaspersky Anti-Virus geladene Objekte werden an das Subsystem für die Virenprüfung übertragen und auf vorhandene Bedrohungen überprüft. Hierbei vergleicht das Subsystem die Signaturen der Objekte mit den Datenbankeinträgen in Kaspersky Anti-Virus und verwendet die heuristische Analyse zum Auffinden unbekannter Viren. Jedem einzelnen Objekt wird nach der Überprüfung ein Status zugewiesen, von dem abhängt, welche nachfolgenden Aktionen für das Objekt vorgenommen werden. Vor dem Sperren oder Ändern eines Objekts kann dieses Im Backup-Ordner gespeichert und so bei Bedarf später in seiner ursprünglichen Form wiederhergestellt werden. Informationen zu beschädigten Objekten werden in einer Datenbank gespeichert und können dort über die Subsysteme für Berichtserstellung und Monitoring abgerufen werden.

- **Subsystem für Updates**: Programmkomponente für die Aktualisierung der Datenbanken von Kaspersky Anti-Virus durch Herunterladen aktueller Daten von den Kaspersky Lab Updateservern oder anderen ausgewählten Quellen. Die Prüfung der vorhandenen Datenbanken auf Aktualität kann automatisch nach einem voreingestellten Zeitplan oder auch manuell erfolgen.

- **Backup-Ordner**: Datenbank auf demselben Computer, auf dem die Programmkomponenten von Kaspersky Anti-Virus installiert sind. Diese enthält Kopien von gefährlichen Objekten vor deren Verarbeitung und Informationen zu diesen Objekten. Die Objekte werden in einem speziellen Format gespeichert und stellen so keine Bedrohung für die Sicherheit der betreffenden Client-Computer dar. Die Objekte aus dem Backup-Ordner können bei Bedarf später wiederhergestellt oder auch gelöscht werden.

- **Subsystem für Berichtserstellung** – Komponente zum Erstellen von Ergebnisberichten zum Virenschutz. Die Berichte werden automatisch anhand eines voreingestellten Zeitplanes oder auf Benutzeranfrage erstellt (manuelles Erstellen von Berichten).

- **Subsystem für Monitoring** – Programmkomponente zum Anzeigen von Informationen über den Programmstatus in Echtzeit: Beschreibung von Programmfunktionen, Ausführungsstatus für Filter und das

Virenprüfungsmodul. Außerdem liefert das Monitoringmodul statistische Informationen zu den überprüften Objekten.

- **Subsystem Diagnose** – diese Komponente führt Journale zum Ausführungsstatus für sämtliche Programmkomponenten. Die entsprechenden Daten werden in Textdateien gespeichert.

- **Subsystem Konsole** – spezielles Programm, über das die Ausführung von Kaspersky Anti-Virus gesteuert und kontrolliert wird. Die Management-Konsole kann entweder auf einem Computer mi Microsoft ISA Server / Forefront TMG oder auf einem separaten Computer installiert werden, der Zugriff auf den Server hat. Falls mehrere Administratoren das Programm gemeinsam verwalten, muss die Management-Konsole auf jedem ihrer Computer installiert sein.

Schematisch kann die Funktionsweise des Programms folgendermaßen dargestellt werden (s. Abb. unten):

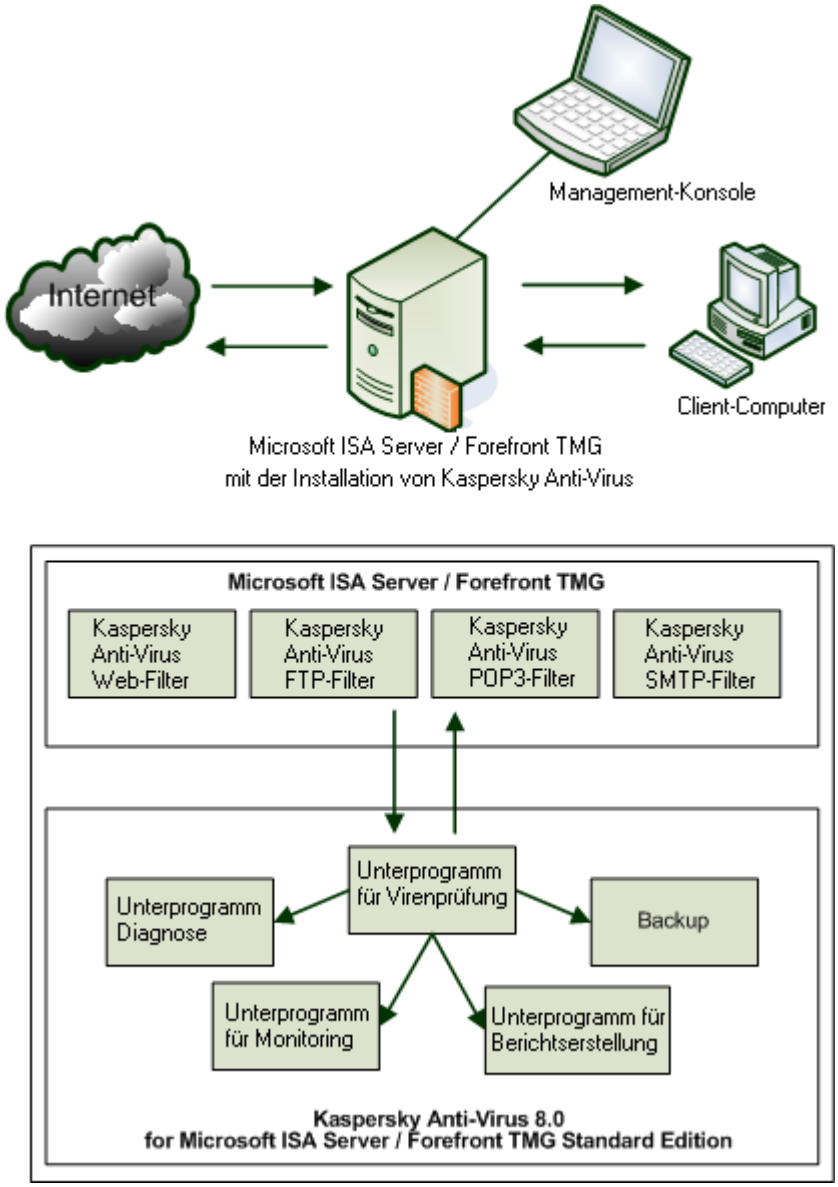

Abbildung 1. Funktionsschema des Programms

SCHUTZ FÜR CLIENT-COMPUTER INSTALLIEREN

Um den Schutz für die Client-Computer innerhalb eines Netzwerkes zu installieren, gehen Sie folgendermaßen vor:

1. Installieren Sie Kaspersky Anti-Virus auf einen Server Microsoft ISA Server / Forefront TMG.
2. Verbinden Sie die Management-Konsole mit dem Server (s. Abschnitt "Management-Konsole mit dem Server verbinden" ab S. 29).
3. Installieren Sie die Lizenz (s. Abschnitt "Programm aktivieren" ab S. 22).
4. Passen Sie den Schutz an:
   - Passen Sie die Einstellungen für Datenbankupdates an (ab S. 33).
   - Passen Sie die Einstellungen für die Virenprüfung an (s. Abschnitt "Virenprüfung" ab S. 39).
   - Passen Sie die Verarbeitungsrichtlinien für Objekte an (s. Abschnitt "Richtlinien für die Virenprüfung pflegen" ab S. 44).
   - Passen Sie die Funktionseinstellungen für Ereignisjournale an (s. Abschnitt "Diagnose" ab S. 66).
5. Überprüfen Sie die Richtigkeit der eingestellten Einstellungen und die korrekte Funktionsweise des Programms mithilfe des Test"virus" EICAR (s. Abschnitt "Richtigkeit der Programmeinstellungen überprüfen" ab S. 30).

Der Serverschutz vor schädlichen Programmen wird automatisch beim Start von Microsoft ISA Server / Forefront TMG aktiviert.

Folgende Maßnahmen sind erforderlich, um zu gewährleisten, dass der Virenschutz für den über die angeschlossenen Client-Computer laufenden E-Mail-Verkehr stets auf dem aktuellen Stand ist:

- regelmäßiges Update der Antiviren-Datenbanken (s. Abschnitt "Datenbanken aktualisieren" ab S. 33);
- Überwachung der Funktion von Kaspersky Anti-Virus überwachen (s. Abschnitt "Funktion von Kaspersky Anti-Virus überwachen" ab S. 58);
- Regelmäßige Prüfung der Ausführungsberichte für das Programm (s. Abschnitt "Berichte" ab S. 54);
- Verarbeiten von Benachrichtigungen;
- Verarbeiten und Bereinigen der Objekte im Backup-Ordner (s. Abschnitt "Backup-Ordner" ab S. 61).

PROGRAMM INSTALLIEREN

Die Installation von Kaspersky Anti-Virus erfolgt mithilfe des Installationsassistenten (s. Abschnitt "Programminstallation" ab S. 13). Vor Beginn sollten Sie die Informationen zur Vorbereitung der Programminstallation aufmerksam lesen (s. Abschnitt "Programminstallation vorbereiten" ab S. 13).

IN DIESEM ABSCHNITT

Programminstallation vorbereiten 13

Aktualisierung von Vorgängerversionen 13

Vorgehen bei der Installation 13

Programm aktivieren. Verschiedene Methoden zur Aktivierung des Programms 18

Änderungen am System nach Installation des Programms 18

Vorbereitung zur Verwendung des Programms 19

Programm wiederherstellen 19

Programm deinstallieren 20

Abschlusseinrichtungsassistent 20

PROGRAMMINSTALLATION VORBEREITEN

Überzeugen Sie sich vor der Installation von Kaspersky Anti-Virus davon, dass Ihr System allen angegebenen Hardware- und Softwareanforderungen entspricht (s. Abschnitt "Hardware- und Softwareanforderungen" ab S. 7). Überzeugen Sie sich außerdem davon, dass der Benutzername, unter dem die Anmeldung am System erfolgt, über die erforderlichen Schreibberechtigungen für die Konfiguration von Microsoft ISA Server / Forefront TMG verfügt.

AKTUALISIERUNG VON VORGÄNGERVERSIONEN

Aktualisierung von Vorgängerversionen. Falls auf Ihrem Computer frühere Versionen des Programms installiert sind, müssen diese vor Installation der neuen Version deinstalliert werden.

VORGEHEN BEI DER INSTALLATION

Um Kaspersky Anti-Virus auf Ihrem Computer zu installieren, starten Sie die ausführbare Datei im Programmpaket. Wenn Sie die Installation in einem Betriebssystem mit aktivierter Benutzerkontensteuerung (User Account Control, UAC) ausführen, müssen Sie die ausführbare Datei als Administrator starten.

Der Installer ist wie ein Assistent aufgemacht. In jedem Fenster sind verschiedene Schaltflächen abgebildet, um den Installationsvorgang zu verwalten.

- **Weiter**: Aktion bestätigen und zum nächsten Schritt im Installationsvorgang wechseln;
- **Zurück**: Zum vorherigen Installationsschritt wechseln;

- **Abbrechen**: Installation abbrechen;
- **Installieren**: Kopieren von Dateien auf die Festplatte und Registrierung der Programmkomponenten starten;
- **Fertig**: Installation des Programms abschließen.

Betrachten wir die einzelnen Schritte des Installationsvorgangs ausführlich.

IN DIESEM ABSCHNITT

Schritt 1. Überprüfen des Systems bezüglich der Installationsvoraussetzungen 14

Schritt 2. Begrüßungsfenster des Installationsassistenten 14

Schritt 3. Lesen des Lizenzvertrags 14

Schritt 4. Installationstyp auswählen 15

Schritt 5. Benutzerdefinierte Installation 15

Schritt 6. Datenspeicherordner auswählen 16

Schritt 7. Regel für Remoteverwaltung anpassen 17

Schritt 8. Dateien kopieren und Programmkomponenten registrieren 17

Schritt 9. Installationsvorgang abschließen 17

SCHRITT 1. ÜBERPRÜFEN DES SYSTEMS BEZÜGLICH DER INSTALLATIONSVORAUSSETZUNGEN

Im ersten Installationsschritt überprüft der Assistent, ob das installierte Betriebssystem und die entsprechenden Updates (Service Packs) den Softwareanforderungen für die Installation von Kaspersky Anti-Virus entsprechen. Außerdem wird überprüft, ob auf dem Computer weitere für die ordnungsgemäße Funktion von Kaspersky Anti-Virus erforderliche Programme installiert sind. Der Installationsassistent überprüft weiterhin, ob auf dem Computer Microsoft ISA Server / Forefront TMG installiert ist und startet die Dienste von Microsoft ISA Server Control (isactrl) und Microsoft ISA Server Storage(isastg), falls diese installiert sind aber noch nicht gestartet wurden.

Wenn eine Bedingung nicht eingehalten wird, erscheint auf dem Bildschirm eine entsprechende Meldung. Bevor Sie mit der Installation von Kaspersky Anti-Virus beginnen, sollten Sie die erforderlichen Service Packs über Windows Update sowie weitere erforderliche Programme installieren.

SCHRITT 2. BEGRÜßUNGSFENSTER DES INSTALLATIONSASSISTENTEN

Erfüllt Ihr System alle erforderlichen Voraussetzungen, öffnet sich nach dem Start der Installationsdatei das Begrüßungsfenster mit einer Meldung, dass die Installation von Kaspersky Anti-Virus gestartet wurde. Zum Fortsetzen der Installation klicken Sie auf die Schaltfläche **Weiter**. Klicken Sie auf die Schaltfläche **Abbrechen**, um das Installationsprogramm zu beenden.

SCHRITT 3. LESEN DES LIZENZVERTRAGS

Im nächsten Fenster der Installation wird der Lizenzvertrag angezeigt, den Sie mit Kaspersky Lab ZAO abschließen. Bitte lesen Sie den Vertrag aufmerksam. Wenn Sie mit sämtlichen Punkten einverstanden sind, setzen Sie das

Kennzeichen bei **Ich akzeptiere die Bedingungen des Lizenzvertrages**, und klicken Sie auf die Schaltfläche **Weiter**. Die Installation wird fortgesetzt.

Zum Ablehnen klicken Sie auf die Schaltfläche **Abbrechen**.

SCHRITT 4. INSTALLATIONSTYP AUSWÄHLEN

An dieser Stelle müssen Sie den gewünschten Installationstyp auswählen. Es sind zwei Varianten für die Installation vorgesehen:

- **Vollständig**. Wählen Sie diese Variante, wenn Sie alle Programmkomponenten installieren möchten. In diesem Fall werden die mit dem Server Microsoft ISA Server / Forefront TMG integrierten Komponenten von Kaspersky Anti-Virus und die Management-Konsole installiert. Diese Variante ist nur verfügbar, wenn auf dem Computer, auf dem der Installationsassistent ausgeführt wird, auch Microsoft ISA Server / Forefront TMG installiert ist.

- **Management-Konsole**. Wählen Sie diese Variante, wenn Sie nur die Management-Konsole für das Programm installieren möchten, ohne die mit dem Server Microsoft ISA Server / Forefront TMG integrierten.Komponenten von Kaspersky Anti-Virus zu installieren. Diese Variante ist von Vorteil, wenn Sie auf einem lokalen Computer das Administrationstool für die Remoteverwaltung von Kaspersky Anti-Virus installieren möchten.

Um den gewünschten Installationstyp auszuwählen, klicken Sie auf die Schaltfläche mit dem entsprechenden Namen.

SCHRITT 5. BENUTZERDEFINIERTE INSTALLATION

Wenn Sie im vorherigen Schritt als Installationstyp **Vollständig** gewählt haben, werden im Fenster **Benutzerdefinierte Installation** automatisch alle Komponenten für die Installation auf die lokale Festplatte ausgewählt.

In der Komponentenstruktur werden folgende Knoten angezeigt:

- **Service**: Dieser Knoten enthält Informationen zu Komponenten von Kaspersky Anti-Virus, die für den Schutz der über Microsoft ISA Server / Forefront TMG übertragenen Daten verantwortlich sind. Um einen ordnungsgemäßen Schutz zu gewährleisten, müssen in Microsoft ISA Server / Forefront TMG bestimmte Filter zum Abfangen der über die entsprechenden Berichte übertragenen Daten integriert werden. Wählen Sie in der Komponente **Service** einen oder mehrere der verfügbaren Filter aus.

- **Filter** – über diesen Knoten können Sie Anti-Viren-Filter auswählen und aktivieren. Folgende Filter stehen Ihnen zur Verfügung:

  - **Web** – Filter zum Abfangen des Datenstroms via HTTP-Protokoll;

  - **FTP** – Filter zum Abfangen des Datenstroms via FTP-Protokoll;

  - **SMTP** – Filter zum Abfangen des Datenstroms via SMTP-Protokoll;

  - **POP3** – Filter zum Abfangen des Datenstroms via POP3-Protokoll;

- **Management-Konsole** – Knoten für die Installation des Tools Management-Konsole zur Verwaltung von Kaspersky-Anti-Virus.

  Die Management-Konsole ist unbedingt erforderlich, damit Sie Kaspersky Anti-Virus verwenden können, und wird unabhängig vom gewählten Installationstyp für das Programm in jedem Fall installiert. Sie können Kaspersky Anti-Virus nicht installieren, ohne die Management-Konsole zu installieren.

Um den Ordner für die Installation der gewünschten Komponenten auszuwählen, gehen Sie folgendermaßen vor:

1. Wählen Sie den Hauptknoten der Komponentenstruktur **Alle Komponenten**.

2. Klicken Sie auf die Schaltfläche **Auswahl**, um das Fenster für die Auswahl des Installationsordners zu öffnen.

3. Geben Sie im Feld **Ordnername** den Pfad für den Ordner vor, in den die gewünschten Komponenten installiert werden sollen. Das Programm muss auf den gleichen Datenträger installiert werden, wie Microsoft ISA Server / Forefront TMG.

4. Klicken Sie auf die Schaltfläche **OK**.

Wenn Sie in der Struktur auf eine der Komponenten klicken, wird Ihnen angezeigt, wie viel freier Speicherplatz für deren Installation auf dem Datenträger benötigt wird. Im rechten Bereich des Fensters für den Installationsassistenten werden ihnen die Größe des benötigten Speicherplatzes und eine kurze Beschreibung zur Funktion der jeweiligen Komponente angezeigt.

- *Um Detailinformationen zum freien Speicherplatz auf einzelnen logischen Datenträgern Ihres Computers zu erhalten, gehen Sie folgendermaßen vor:*

1. Klicken Sie auf die Schaltfläche **Datenträger**.

2. Die gewünschten Informationen werden Ihnen im Fenster **Erforderlicher Speicherplatzt auf dem Datenträger** angezeigt.

3. Um das Fenster zu schließen, klicken Sie auf **OK**.

- *Um eine Komponente für die Installation auszuwählen, gehen Sie folgendermaßen vor:*

1. Öffnen Sie durch Klick mit der linken Maustaste das Menü für den Knoten der gewünschten Komponente.

2. Wählen Sie **Wird zum Starten von der Festplatte installiert** oder **Alle Komponenten**.

   Wenn Sie **Alle Komponenten** wählen, wird die gewünschte Komponente einschließlich aller ihrer Unterkomponenten für die Installation vorbereitet.

Soll eine Komponente nicht installiert werden, müssen Sie im Kontextmenü den Punkt **Die Komponente wird nicht verfügbar sein** wählen.

Klicken Sie auf die Schaltfläche **Weiter**, um die Installation fortzusetzen. Wenn Sie sich im vorherigen Schritt entschieden haben, nur die Management-Konsole zu installieren, fahren Sie bitte mit Schritt 9 fort.

SCHRITT 6. DATENSPEICHERORDNER AUSWÄHLEN

An dieser Stelle müssen Sie einen Ordner auf der Festplatte auswählen, in dem die bei der Ausführung des Programms generierten Daten gespeichert werden sollen. Folgende Daten werden in diesem Ordner gespeichert:

- Journale zur Programmausführung und zum Virenschutz;
- Hilfsdaten und temporäre Daten, die benötigt werden, um die ordnungsgemäße Funktion des Programms und einen ununterbrochenen stabilen Virenschutz zu gewährleisten;
- Anti-Viren-Datenbanken für die Suche nach bekannten Viren und schädlichen Programmen;
- Berichte;
- Die Statistik-Datenbank;
- Die Datenbank für die Dateiablage;
- Die Datenbank für den Backup-Ordner;
- Sonstige für die Interaktion mit dem Server für Microsoft ISA Server / Forefront TMG erforderliche Daten.

Im Feld **Datenordner** wird der Pfad für den standardmäßig verwendeten Speicherordner für Programmdaten angezeigt.

- *Um einen anderen Pfad für den Datenspeicherordner von Kaspersky Anti-Virus zu wählen,*

  geben Sie den Pfad im Feld **Datenordner** ein, oder wählen Sie den gewünschten Ordner im Fenster **Aktuellen Zielordner ändern** durch Klick auf die Schaltfläche **Ändern**.

Bei Bedarf können Sie nach der Installation von Kaspersky Anti-Virus den Speicherort für den Programmdatenordner ändern (s. Abschnitt "Speicherort für den Programmdatenordner ändern" ab S. 68).

Zum Fortsetzen der Installation klicken Sie auf die Schaltfläche **Weiter**.

SCHRITT 7. REGEL FÜR REMOTEVERWALTUNG ANPASSEN

An dieser Stelle müssen Sie den Port vorgeben, über den sich die auf einem Remotecomputer installierte Management-Konsole für die Programmverwaltung mit Kaspersky Anti-Virus verbinden soll.

Geben Sie die Nummer für den Port im Feld **TCP-Port** ein. Der voreingestellte Standardwert beträgt – 5000.

Ist das Häkchen **Regel aktivieren** gesetzt, erstellt der Installationsassistent in der Richtlinie der Firewall des Servers Microsoft ISA Server / Forefront TMG eine benutzerdefinierte Regel, die eingehende Verbindungen zu dem gewählten Serverport zulässt. Die Option zur Remoteverwaltung von Kaspersky Anti-Virus wird automatisch aktiviert. Entfernen Sie das Häkchen, wenn Sie nicht sofort nach der Programminstallation die Remoteverwaltung erlauben möchten.

Zum Fortsetzen der Installation klicken Sie auf die Schaltfläche **Weiter**.

SCHRITT 8. DATEIEN KOPIEREN UND PROGRAMMKOMPONENTEN REGISTRIEREN

In diesem Schritt werden Dateien in den Installationsordner auf Ihrem Computer kopiert, den Sie im Auswahlfenster für Programmkomponenten ausgewählt haben (s. Abschnitt "Schritt 5. Benutzerdefinierte Installation" ab S. 15); außerdem werden die installierten Programmkomponenten in die Registry des Betriebssystems eingetragen und mit dem Server Microsoft ISA Server / Forefront TMG integriert.

Zum Fortsetzen der Installation klicken Sie auf die Schaltfläche **Installieren**. Anschließend startet der Assistent die Installation des Programms. Klicken Sie auf die Schaltfläche **Zurück**, falls Sie in den vorherigen Fenstern des Assistenten festgelegte Einstellungen ändern möchten.

Während der Installation und Registrierung der Filter müssen Sie die Dienste für den Server Microsoft ISA Server / Forefront TMG neu starten. Klicken Sie auf die Schaltfläche **OK** im Meldungsfenster, um die Dienste neu zu starten, die für die korrekte Integration von Kaspersky Anti-Virus auf dem Server für Microsoft ISA Server / Forefront TMG erforderlich sind.

Während der Installation von Kaspersky Anti-Virus werden einige Dienste von Microsoft ISA Server / Forefront TMG neu gestartet. Dadurch können bestehende Verbindungen zu Client-Computern unterbrochen werden.

Wenn Sie im Fenster mit der Aufforderung zum Neustart der Dienste auf die Schaltfläche **Abbrechen** klicken, wird die Installation beendet. In diesem Fall werden sämtliche durch das Installationsprogramm bereits ausgeführten Schritte zur Installation von Kaspersky Anti-Virus rückgängig gemacht. Die Installation des Programms wird abgebrochen.

SCHRITT 9. INSTALLATIONSVORGANG ABSCHLIEßEN

Im Fenster **Installation wird abgeschlossen** werden Sie informiert, dass die Installation von Kaspersky Anti-Virus abgeschlossen wird.

Setzen Sie das Häkchen **Einrichtungsassistenten starten**, um sofort nach Abschluss des Installationsassistenten den Abschlusseinrichtungsassistenten zu starten (s. Abschnitt "Abschlusseinrichtungsassistent" ab S. 20). Mithilfe des Abschlusseinrichtungsassistenten können Sie sofort nach der Installation des Programms die Schlüsseldateien mit

Lizenzen zum Programm installieren. Dies ist kein obligatorischer Schritt. Die über diesen Assistenten festgelegten Einstellungen können Sie später über die Management-Konsole jederzeit wieder ändern.

Klicken Sie auf die Schaltfläche **Fertig**, um das Fenster des Installationsassistenten zu schließen.

Im Hauptmenü wird die Programmgruppe **Kaspersky Anti-Virus 8.0 für Microsoft ISA Server und Forefront TMG Standard Edition** angezeigt, aus der Sie die Management-Konsole des Programms starten und das Hilfesystem aufrufen können.

PROGRAMM AKTIVIEREN. VERSCHIEDENE METHODEN ZUR AKTIVIERUNG DES PROGRAMMS

Damit Kaspersky Anti-Virus für den Virenschutz der angeschlossenen Client-Computer aktuelle Anti-Viren-Datenbanken verwenden kann, müssen Sie das Programm zuvor aktivieren. "Aktivieren" bedeutet Hinzufügen der Datei mit dem Lizenzschlüssel zum Programm.

Sie können das Programm auf zwei Arten aktivieren:

- Mithilfe des Abschlusseinrichtungsassistenten (s. Abschnitt "Abschlusseinrichtungsassistent" ab S. 20).
- Mithilfe der Management-Konsole (s. Abschnitt "Lizenzverwaltung" ab S. 22).

ÄNDERUNGEN AM SYSTEM NACH INSTALLATION DES PROGRAMMS

Während der Installation werden folgende Ordner angelegt:

- **Installationsordner**: <ProgramFiles>\Kaspersky Lab\Kaspersky Anti-Virus 8.0 für Microsoft ISA Server und Forefront TMG Standard Edition, wobei <ProgramFiles> folgende Werte annehmen kann:
  - Ist Microsoft ISA / Forefront TMG auf den gleichen Datenträger installiert wie Microsoft Windows, so ist <ProgramFiles> der Standardordner Program Files, deren Pfad in der Systemvariablen %ProgramFiles% für 32-Bit-Systeme oder %ProgramFiles(x86)% für 64-Bit-Systeme gespeichert ist;
  - Ist Microsoft ISA / Forefront TMG auf einen Datenträger ohne Microsoft Windows installiert, wird der Ordner <ProgramFiles> an der Stelle <Datenträger Microsoft ISA / Forefront TMG>:\Program Files angelegt.
- **Datenordner**: <CommonAppDataFolder>\Kaspersky Anti-Virus 8.0 für Microsoft ISA Server und Forefront TMG Standard Edition\data. Hierbei ist <CommonAppDataFolder> der von allen Benutzern verwendete Ordner **Common AppData** für die betreffenden Anwendungen. Den genauen Wert für **Common AppData** finden Sie im Schlüssel der Registry: **[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders]**
- **Ordner für gemeinsam genutzte Komponenten (ISD)**: <CommonFilesFolder>\Kaspersky Lab\ISD>. Hierbei ist <CommonFilesFolder> der Standardordner Common Files für 32-Bit-Programme für den aktuellen Benutzer. Der Ordnerpfad ist in der Systemvariablen %CommonProgramFiles% für 32-Bit-Systeme bzw. %CommonProgramFiles(x86)% für 64-Bit-Systeme gespeichert.
- **Ordner im Startmenü**: <ProgramMenuFolder>\Kaspersky Anti-Virus 8.0 für Microsoft ISA Server und Forefront TMG Standard Edition. Hierbei ist <ProgramMenuFolder> der Ordner **Common Programs**, der die Elemente des Menüs **Start** für alle Benutzer enthält. Den genauen Wert für **Common Programs** finden Sie im Schlüssel der Registry: **[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders]**
- **Ordner in Downloaded Installations**: <DownloadedInstallationsFolder>\{0D40E22B-2FB4-4237-AB63-3FFA9A4CE2EA}. Hierbei ist <DownloadedInstallationsFolder> der Standardordner Downloaded Installations

zum Speichern von Installationsdateien mit dem Pfad %WinDir%\Downloaded. %WinDir% ist hierbei der Ordner, in dem sich Microsoft Windows befindet.

Während der Installation werden außerdem folgende Aktionen ausgeführt:

- Zusätzlich werden folgende Programme installiert: Microsoft Windows Installer 3.1, Microsoft Visual C++ 2005 Redistributable Package (x86).
- Der Service **Kaspersky Anti-Virus 8.0 für Microsoft ISA Server und Forefront TMG SE** (kavisasrv.exe) wird in die Registry eingetragen.
- Auf dem Server für Microsoft ISA Server / Forefront TMG wird eine Regel für die Firewall erstellt, die den Remotezugriff auf den Computer mit der Installation von Kaspersky Anti-Virus durch die Management-Konsole erlaubt.
- Es werden zwei Gruppen von Performanceindikatoren hinzugefügt: **KAV for ISA and TMG Filter** und **KAV für ISA und TMG Service**.
- Das Benachrichtigungstool für Ereignisse von Kaspersky Anti-Virus wird in Microsoft ISA Server / Forefront TMG registriert.

Die Änderungen in der Registry von Microsoft Windows für 32-Bit- und 64-Bit-Versionen sind in Anlage 1 beschrieben.

VORBEREITUNG ZUR VERWENDUNG DES PROGRAMMS

Direkt nach der Installation verwendet Kaspersky Anti-Virus eine Minimalauswahl an standardmäßigen Grundeinstellungen, die von Kaspersky Lab empfohlen werden. Bei Bedarf können Sie diese Grundeinstellungen ändern und zusätzliche Einstellungen vornehmen, um besonderen Eigenschaften Ihres Netzwerkes und des Computers Rechnung zu tragen, auf dem Microsoft ISA Server / Forefront TMG installiert ist.

Das Anpassen der Funktionseinstellungen für das Programm erfolgt über den Arbeitsplatz des Administrators. Dies ist der Computer, auf dem die Komponente **Management-Konsole** installiert ist.

Wir empfehlen dringend, den Computer für stündliche automatische Datenbankupdates anzupassen (s. Abschnitt "Datenbanken aktualisieren" ab S. 34).

Um sich von der ordnungsgemäße Funktion des Programms zu überzeugen, können Sie den Schutz mithilfe von Testviren überprüfen (s. Abschnitt "Korrekte Programmeinstellungen überprüfen" ab S. 30).

Um die Ausführung von Kaspersky Anti-Virus zu kontrollieren, verwenden Sie den Knoten **Monitoring** (s. Abschnitt "**Monitoring der Programmfunktionen**" ab S. 58).

PROGRAMM WIEDERHERSTELLEN

Falls bei der Erstinstallation von Kaspersky Anti-Virus oder bei der Registrierung der Komponenten Fehler auftreten oder ausführbare Dateien beschädigt wurden, können Sie das Programm wiederherstellen.

Um das Programm erneut zu installieren, starten Sie nochmals die ausführbare Datei im Installationspaket. Sie können hierzu auch den Assistenten zum Installieren und Deinstallieren von Programmen unter Microsoft Windows verwenden.

➧ *Um den Assistenten zum Installieren und Deinstallieren von Programmen unter Microsoft Windows zu verwenden, gehen Sie folgendermaßen vor:*

1. Öffnen Sie das Fenster **Programme installieren und deinstallieren**. Um dieses Fenster zu öffnen, haben Sie zwei Möglichkeiten:

   a. Drücken Sie die Tastenkombination **WINDOWS + R**;

b. Führen Sie in dem erscheinenden Dialogfenster **Ausführen** den Befehl appwiz.cpl aus, und drücken Sie **ENTER**.

2. Suchen Sie im Fenster **Programme installieren und deinstallieren** den Eintrag für Kaspersky Anti-Virus und markieren Sie ihn.

3. Klicken Sie auf **Ändern / Deinstallieren**.

4. Klicken Sie in dem folgenden Fenster des Assistenten auf die Schaltfläche **Weiter**.

5. Klicken Sie auf die Schaltfläche **Wiederherstellen** im nächsten Fenster des Assistenten.

6. Klicken Sie auf die Schaltfläche **Ändern** im nächsten Fenster des Installationsassistenten für Kaspersky Anti-Virus, und warten Sie, bis die Neuinstallation abgeschlossen ist. Bei der erneuten Registrierung und Integration der Programmkomponenten auf dem Server für Microsoft ISA Server / Forefront TMG überschreibt der Assistent automatisch die bereits installierten Programmdateien.

PROGRAMM DEINSTALLIEREN

Um Kaspersky Anti-Virus zu deinstallieren, verwenden Sie die entsprechenden Standardtools unter Microsoft Windows oder das Installationspaket. Hierbei werden sämtliche installierten Programmkomponenten vom Computer entfernt.

ABSCHLUSSEINRICHTUNGSASSISTENT

Mithilfe des Abschlusseinrichtungsassistenten können Sie sofort nach der Installation des Programms die Schlüsseldateien mit Lizenzen zum Programm installieren. Der Abschlusseinrichtungsassistent wird sofort nach der Installation automatisch gestartet, sofern Sie im letzten Schritt des Einrichtungsassistenten das Kästchen **Abschlusseinrichtungsassistenten starten** aktiviert haben.

In jedem Fenster stehen verschiedene Schaltflächen, um den Installationsvorgang zu verwalten.

- **Weiter** – Vorgang wird angenommen und es geht weiter zum nächsten Schritt im Installationsvorgang.
- **Zurück** – zum vorherigen Schritt des Assistenten wechseln;
- **Abbrechen** – Fenster des Assistenten schließen, ohne die Änderungen zu speichern;
- **Fertig** – den Assistenten beenden, Änderungen speichern und Fenster schließen.

Im ersten Fenster des Abschlusseinrichtungsassistenten, **Hauptlizenzschlüssel hinzufügen**, können Sie den Schlüssel für die Hauptlizenz installieren.

Um den Schlüssel für die Hauptlizenz zum Programm hinzuzufügen, gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Schaltfläche **Hinzufügen / Ersetzen**, und wählen Sie in dem folgenden Fenster die Datei mit dem gültigen Lizenzschlüssel aus (Dateierweiterung für Schlüsseldateien: *.key).

2. Nach dem Hinzufügen des Schlüssels erscheint auf dem Bildschirm folgende Meldung:

   - Lizenztyp;
   - Lizenzinhaber;
   - Anzahl Benutzer;
   - Ablauf der Gültigkeitsdauer für die Lizenz;
   - Seriennummer der Lizenz;

Im zweiten Fenster des Abschlusseinrichtungsassistenten, **Reservelizenzschlüssel hinzufügen**, können Sie den Schlüssel für die Reservelizenz installieren.

Um den Reserveschlüssel für die Hauptlizenz zum Programm hinzuzufügen, gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Schaltfläche **Hinzufügen / Ersetzen**, und wählen Sie in dem folgenden Fenster die Datei mit dem gültigen Lizenzschlüssel aus (Dateierweiterung für Schlüsseldateien: *.key).

2. Nach dem Hinzufügen des Schlüssels erscheint auf dem Bildschirm folgende Meldung:

   - Anzahl Benutzer;
   - Ablauf der Gültigkeitsdauer für die Lizenz;
   - Seriennummer der Lizenz;

3. Der Reserveschlüssel wird automatisch zum aktiven Schlüssel, sobald die Gültigkeitsdauer des aktiven Schlüssels abgelaufen ist.

LIZENZVERWALTUNG

Um zu gewährleisten, dass Kaspersky Anti-Virus für den Virenschutz der Client-Computers stets aktuelle Anti-Viren-Datenbanken verwendet, benötigen Sie eine Lizenz (s. Abschnitt "Programm aktivieren" ab S. 22).

Ist keine Lizenz installiert, wird der über Microsoft ISA Server / Forefront TMG verlaufende E-Mail-Verkehr nicht überwacht, und es werden keine Updates für die Anti-Viren-Datenbanken ausgeführt.

Ist die Lizenz abgelaufen, überwacht Kaspersky Anti-Virus den Datenstrom mithilfe der bereits installierten Anti-Viren-Datenbanken. Es werden jedoch keine Updates ausgeführt. Wir empfehlen Ihnen eine Benachrichtigung zum Ablauf der Gültigkeitsdauer für die Lizenz einzurichten (s. Abschnitt "Benachrichtigung zum Ablauf der Lizenz einrichten24" ab S.).

Befindet sich die Lizenz auf der "Blacklist", wird der über Microsoft ISA Server / Forefront TMG verlaufende E-Mail-Verkehr nicht überwacht. Es werden jedoch Updates der Anti-Viren-Datenbanken ausgeführt.

Für das Programm können zwei Lizenzschlüssel gleichzeitig installiert werden: ein aktiver und ein Reserveschlüssel. Nach Ablauf der Gültigkeitsauer für den aktuell aktiven Schlüssel wird der Reserveschlüssel automatisch zum aktiven Schlüssel (s. Abschnitt "Reserveschlüssel hinzufügen" ab S. 23).

IN DIESEM ABSCHNITT

Programm aktivieren 22

Reserveschlüssel hinzufügen 23

Benachrichtigung zum Ablauf der Lizenz anpassen 24

PROGRAMM AKTIVIEREN

Um das Programm, also den Virenschutz für die angeschlossenen Client-Computer durch Anti-Virus, zu aktivieren, müssen Sie einen Schlüssel zum Programm hinzufügen.

Ist keine Lizenz installiert, wird der über Microsoft ISA Server / Forefront TMG verlaufende E-Mail-Verkehr nicht überwacht, und es werden keine Updates für die Anti-Viren-Datenbanken ausgeführt.

Ist die Lizenz abgelaufen, überwacht Kaspersky Anti-Virus den Datenstrom mithilfe der bereits installierten Anti-Viren-Datenbanken. Es werden jedoch keine Updates ausgeführt. Wir empfehlen Ihnen eine Benachrichtigung zum Ablauf der Gültigkeitsdauer für die Lizenz einzurichten (s. Abschnitt "Benachrichtigung zum Ablauf der Lizenz einrichten" ab S. 24).

Befindet sich die Lizenz auf der "Blacklist", wird der über Microsoft ISA Server / Forefront TMG verlaufende Datenstrom nicht überwacht. Es werden jedoch Updates der Anti-Viren-Datenbanken ausgeführt.

Gehen Sie folgendermaßen vor, um das Programm zu aktivieren:

1. Markieren Sie in der Konsolenstruktur den Knoten für den gewünschten Server.
2. Klicken Sie auf die Schaltfläche **Allgemeine Parameter**.
3. Öffnen Se in dem folgenden Fenster **Allgemeine Parameter** die Registerkarte **Lizenzen** (s. Abb. unten).
4. Klicken Sie auf die Schaltfläche **Hinzufügen / Ersetzen**, und wählen Sie in dem folgenden Fenster die Datei mit dem gültigen Lizenzschlüssel aus (Dateierweiterung für Schlüsseldateien: *.key).
5. Nach dem Hinzufügen des Schlüssels erscheint auf dem Bildschirm folgende Meldung:
   - Lizenztyp;

- Lizenzinhaber;
- Anzahl Benutzer;
- Ablauf der Gültigkeitsdauer für die Lizenz;
- Seriennummer der Lizenz;

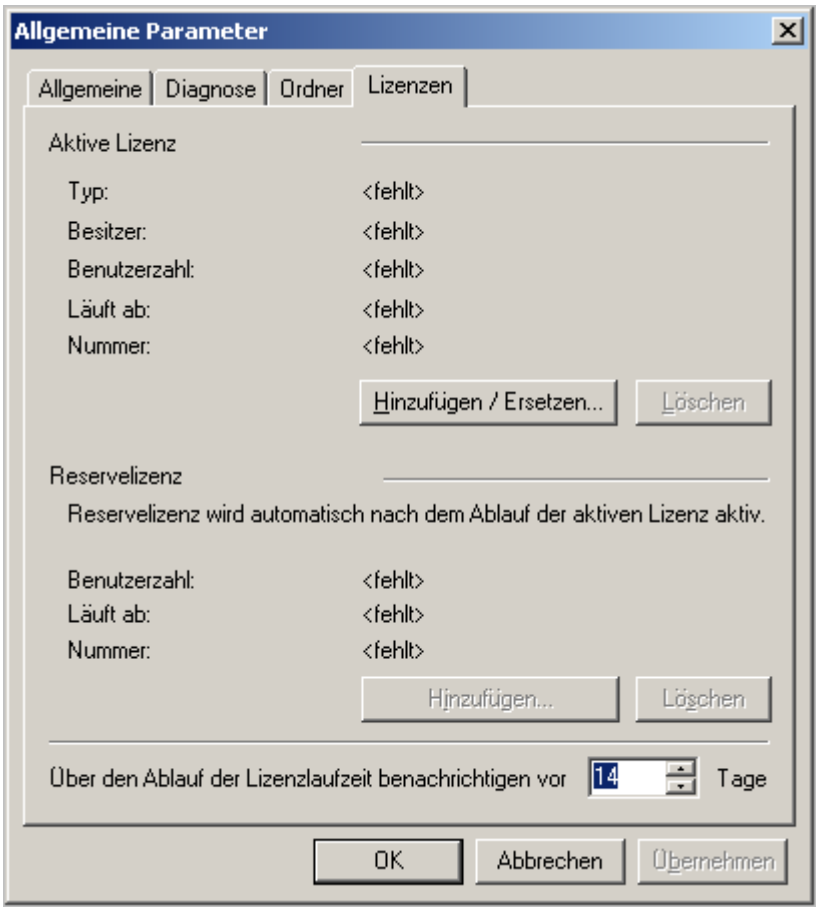

Abbildung 2. Registerkarte "Lizenzen"

RESERVESCHLÜSSEL HINZUFÜGEN

➧ *Um einen Reserveschlüssel hinzuzufügen, gehen Sie folgendermaßen vor:*

1. Markieren Sie in der Konsolenstruktur den Knoten für den gewünschten Server.
2. Klicken Sie auf die Schaltfläche **Allgemeine Parameter**.
3. Öffnen Sie in dem folgenden Fenster **Allgemeine Parameter** die Registerkarte **Lizenzen**.
4. Klicken Sie auf die Schaltfläche **Hinzufügen**, in dem folgenden Fenster die Datei mit dem Reserveschlüssel aus (Dateierweiterung für Schlüsseldateien: *.key).
5. Nach dem Hinzufügen des Schlüssels erscheint auf dem Bildschirm folgende Meldung:
   - Anzahl Benutzer;
   - Ablauf der Gültigkeitsdauer für die Lizenz;

- Seriennummer der Lizenz;

6. Der Reserveschlüssel wird automatisch zum aktiven Schlüssel, sobald die Gültigkeitsdauer des aktiven Schlüssels abgelaufen ist.

BENACHRICHTIGUNG ZUM ABLAUF DER LIZENZ ANPASSEN

Um eine Benachrichtigung zum Ablauf der Gültigkeitsdauer für die Lizenz anzupassen, gehen Sie folgendermaßen vor:

1. Markieren Sie in der Konsolenstruktur den Knoten für den gewünschten Server.
2. Klicken Sie auf die Schaltfläche **Allgemeine Parameter**.
3. Öffnen Sie in dem folgenden Fenster **Allgemeine Parameter** die Registerkarte **Lizenzen**.
4. Geben Sie im Feld **Bei Ablauf der Lizenz N Tage vorher benachrichtigen** die gewünschte Anzahl der Tage ein.
5. Klicken Sie auf die Schaltfläche **OK**, um die vorgenommenen Änderungen zu speichern und das Fenster zu schließen.

PROGRAMMOBERFLÄCHE

Die Management-Konsole für Kaspersky Anti-Virus ist eine Standard- Toolkonsole (MMC) für Microsoft Windows (s. Abschnitt "Programmhauptfenster" ab S. 25).

Das Anpassen der Funktionseinstellungen für Kaspersky Anti-Virus erfolgt über spezielle Einrichtungsfenster (s. Abschnitt "Programmeinrichtungsfenster" ab S. 26).

IN DIESEM ABSCHNITT

Programmhauptfenster 25

Programmeinrichtungsfenster 26

PROGRAMMHAUPTFENSTER

Das Programmhauptfenster ist eine Toolkonsole (MMC) (s. Abb. unten). Um das Programmhauptfenster aufzurufen, klicken Sie auf die Verknüpfung **Management-Konsole** auf dem Desktop.

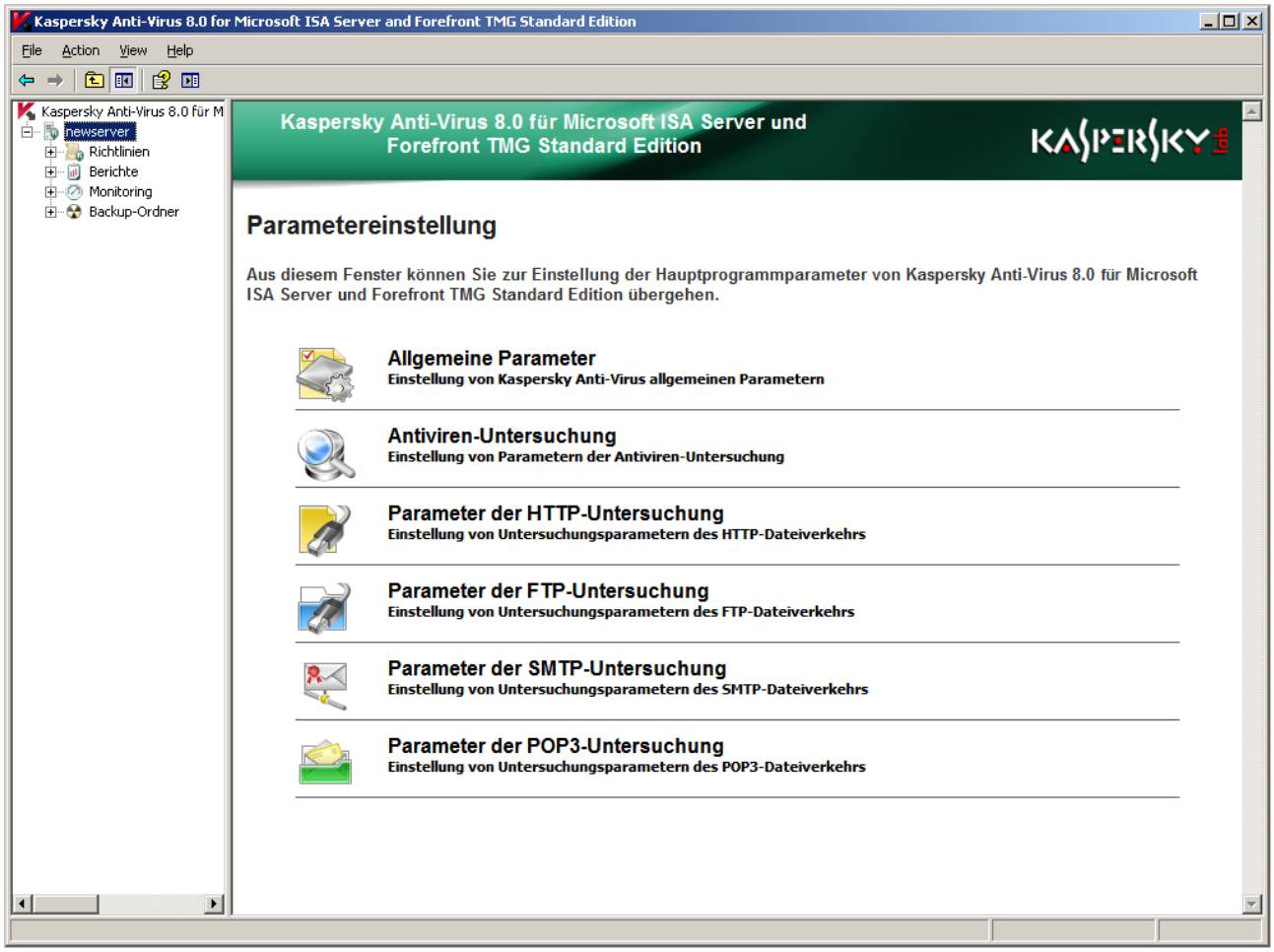
Kaspersky Anti-Virus 8.0 for Microsoft ISA Server and Forefront TMG Standard Edition
File Action View Help
Kaspersky Anti-Virus 8.0 für M
newserver
Richtlinien
Berichte
Monitoring
Backup-Ordner
Kaspersky Anti-Virus 8.0 für Microsoft ISA Server und Forefront TMG Standard Edition
KASPERSKY lab
Parametereinstellung
Aus diesem Fenster können Sie zur Einstellung der Hauptprogrammparameter von Kaspersky Anti-Virus 8.0 für Microsoft ISA Server und Forefront TMG Standard Edition übergehen.
Allgemeine Parameter
Einstellung von Kaspersky Anti-Virus allgemeinen Parametern
Antiviren-Untersuchung
Einstellung von Parametern der Antiviren-Untersuchung
Parameter der HTTP-Untersuchung
Einstellung von Untersuchungsparametern des HTTP-Dateiverkehrs
Parameter der FTP-Untersuchung
Einstellung von Untersuchungsparametern des FTP-Dateiverkehrs
Parameter der SMTP-Untersuchung
Einstellung von Untersuchungsparametern des SMTP-Dateiverkehrs
Parameter der POP3-Untersuchung
Einstellung von Untersuchungsparametern des POP3-Dateiverkehrs

Abbildung 3. Programmhauptfenster

Das Fenster besteht aus zwei Bereichen: der *Konsolenstruktur* und dem *Ergebnisbereich*.

Die *Konsolenstruktur* ist die Hierarchiestruktur im linken Teil des Fensters der MMC. Die Konsolenstruktur enthält die Knoten für die wesentlichsten Programmfunktionen. Den Konsolenstruktur können Sie in der Konsole anzeigen oder verbergen.

Ein *Knoten* ist ein beliebiges Element der Konsolenstruktur, dem Objekte zugeordnet sind. Durch Doppelklick auf das entsprechende Pluszeichen können Sie Knoten expandieren und deren Inhalt anzeigen. Durch Doppelklick auf das Minuszeichen wird der Knoten wieder geschlossen.

Der *Ergebnisbereich* befindet sich im rechten Teil der Toolkonsole. Hier werden Objekte sowie Informationen zu den aktuell in der Konsolenstruktur ausgewählten Elementen angezeigt. Der Ergebnisbereich wird Ihnen stets angezeigt, gleich welche Einstellungen Sie gewählt haben.

Sie können die Ansicht für das Tool individuell anpassen, indem Sie bestimmte Bereiche des Fensters anzeigen bzw. ausblenden.

Zum Anpassen der Ansicht für die Toolkonsole gehen Sie folgendermaßen vor:

1. Öffnen Sie die **Management-Konsole**.
2. Wählen Sie im Menü unter **Ansicht** den Punkt **Anpassen**.
3. Wählen Sie in dem erscheinenden Dialogfenster **Ansicht anpassen** die Elemente aus, die angezeigt werden sollen, indem Sie die entsprechenden Häkchen setzen oder entfernen.

Um Detailinformationen zur Toolschnittstelle aufzurufen, gehen Sie folgendermaßen vor:

1. Öffnen Sie die **Management-Konsole**.
2. Wählen Sie den Menüpunkt **Hilfe**.

PROGRAMMEINRICHTUNGSFENSTER

Die Basiseinstellungen von Kaspersky Anti-Virus können Sie über spezielle Einrichtungsfenster anpassen. Um die Einrichtungsfenster aufzurufen, wählen Sie in der Management-Konsole den Knoten des gewünschten Servers: Im Ergebnisbereich werden Ihnen die Schaltflächen zum Aufrufen der weiteren Einrichtungsfenster angezeigt (s. Abb. unten):

- **Allgemeine Einstellungen**: Einstellungen zum Erstellen von Journalen für Programmfunktionen (s. Abschnitt "Diagnose" ab S. 66), Funktionseinstellungen für Lizenzen (s. Abschnitt "Lizenzverwaltung" ab S. 22).
- **Antiviren-Untersuchung**: Update-Einstellungen für die Datenbanken in Kaspersky Anti-Virus und Performanceeinstellungen des Anti-Viren-Kernels (s. Abschnitt "Virenprüfung" ab S. 39).
- **Einstellungen der HTTP-Untersuchung**: Ändern von Templates zum Ersetzen gesperrter Objekte, Anpassen der Einstellungen für den Datenstrom über HTTP:
  - Maximale Wartezeit bis zum Start der Datenübertragung an Client-Computer;
  - nicht vor Abschluss der Prüfung an die Client-Computer übertragene Datenmenge;
  - Geschwindigkeit für Übertragung nicht geprüfter Objekte an Client-Computer.
- **Einstellungen der FTP-Untersuchung** – maximale Wartezeit bis zum Start der Datenübertragung an Client-Computer und nicht vor Abschluss der Prüfung an die Client-Computer übertragene Datenmenge.
- **Einstellungen der SMTP-Untersuchung** – Ändern von Templates zum Ersetzen von gesperrten Objekten und Betreffzeilen in E-Mails.

- **Einstellungen der POP3-Untersuchung** – Ändern von Templates zum Ersetzen von gesperrten Objekten und Betreffzeilen in E-Mails.

Kaspersky Anti-Virus 8.0 für Microsoft ISA Server und Forefront TMG Standard Edition
KASPERSKY lab
Parametereinstellung
Aus diesem Fenster können Sie zur Einstellung der Hauptprogrammparameter von Kaspersky Anti-Virus 8.0 für Microsoft ISA Server und Forefront TMG Standard Edition übergehen.
Allgemeine Parameter
Einstellung von Kaspersky Anti-Virus allgemeinen Parametern
Antiviren-Untersuchung
Einstellung von Parametern der Antiviren-Untersuchung
Parameter der HTTP-Untersuchung
Einstellung von Untersuchungsparametern des HTTP-Dateiverkehrs
Parameter der FTP-Untersuchung
Einstellung von Untersuchungsparametern des FTP-Dateiverkehrs
Parameter der SMTP-Untersuchung
Einstellung von Untersuchungsparametern des SMTP-Dateiverkehrs
Parameter der POP3-Untersuchung
Einstellung von Untersuchungsparametern des POP3-Dateiverkehrs

Abbildung 4. das Programmkonfigurationsfenster

PROGRAMM STARTEN UND BEENDEN

Nach der Installation des Programms wird automatisch der Dienst **Kaspersky Anti-Virus 8.0 für Microsoft ISA Server und Forefront TMG SE** (kavisasrv.exe) gestartet, der die ordnungsgemäße Funktion von Kaspersky Anti-Virus gewährleistet.

Gehen Sie folgendermaßen vor, um die Arbeit von Kaspersky Anti-Virus anzuhalten:

1. Öffnen Sie die Management-Konsole von **Microsoft ISA Server / Forefront TMG**.
2. Wählen Sie in der Konsolenstruktur der Management-Konsole den Serverknoten aus, anschließend den Knoten **Configuration**, dann den Knoten **Add-ins** für Microsoft ISA Server oder den Knoten **System** für Forefront TMG. Im rechten Teil des Fensters wird nun eine Liste der installierten Filter angezeigt.
3. Deaktivieren Sie in der Registerkarte **Web Filters** den **Kaspersky Anti-Virus Web-Filter**.
4. Deaktivieren Sie in der Registerkarte **Application Filters** die folgenden Programmfilter: **Kaspersky Anti-Virus FTP-Filter**, **Kaspersky Anti-Virus POP3-Filter**, **Kaspersky Anti-Virus SMTP-Filter**.
5. Klicken Sie auf die Schaltfläche **Apply**, um die vorgenommenen Änderungen zu speichern. Wählen Sie im erscheinenden Dialogfenster die Option "Änderungen speichern und Dienst neu starten".
6. Stoppen Sie den Dienst **Kaspersky Anti-Virus 8.0 für Microsoft ISA Server und Forefront TMG** im Servicemanager von Microsoft Windows.

   Kaspersky Anti-Virus wird angehalten.

Wenn Sie Kaspersky Anti-Virus anhalten, aber die Filter in Microsoft ISA Server / Forefront TMG nicht deaktivieren, wird der Dienst einige Zeit nach dem Anhalten automatisch wieder gestartet.

Um Kaspersky Anti-Virus nach dem Anhalten wieder zu starten, gehen Sie folgendermaßen vor:

1. Öffnen Sie die Management-Konsole für **Microsoft ISA Server / Forefront TMG**.
2. Wählen Sie in der Konsolenstruktur der Management-Konsole den Serverknoten aus, anschließend den Knoten **Configuration**, dann den Knoten **Add-ins** für Microsoft ISA Server oder den Knoten **System** für Forefront TMG. Im rechten Teil des Fensters wird nun eine Liste der installierten Filter angezeigt.
3. Aktivieren Sie in der Registerkarte **Application Filters** die folgenden Programmfilter: **Kaspersky Anti-Virus FTP-Filter**, **Kaspersky Anti-Virus POP3-Filter**, **Kaspersky Anti-Virus SMTP-Filter**.
4. Aktivieren Sie in der Registerkarte **Web Filters** den **Kaspersky Anti-Virus Web-Filter**.
5. Nachdem die Filter aktiviert sind, wird der Dienst **Kaspersky Anti-Virus 8.0 für Microsoft ISA Server und Forefront TMG** automatisch gestartet.

MANAGEMENT-KONSOLE MIT DEM SERVER VERBINDEN

Zum verbinden der Management-Konsole mit dem Server gehen Sie folgendermaßen vor:

1. Starten Sie die Management-Konsole. Es öffnet sich das Fenster für die Serververbindung (s. Abb. unten).

2. Markieren Sie das Kästchen **Lokaler Computer**, wenn die Konsole von dem Computer gestartet wurde, auf dem auch Kaspersky Anti-Virus installiert ist, Markieren Sie das Kästchen **Lokaler Computer** und geben Sie im Feld **Name** den entsprechenden Namen im Microsoft Windows-Netzwerk, die IP-Adresse oder den Domainnamen für den Computer ein, auf dem Kaspersky Anti-Virus installiert ist. Über die Schaltfläche **Auswahl** können Sie auch einen Remotecomputer auswählen.

3. Markieren Sie das Kästchen **Daten für aktuelles Benutzerkonto**, wenn der Serverzugriff über das aktuelle Benutzerkonto erfolgt, oder markieren Sie das Kästchen **Anderes Benutzerkonto angeben**, und geben Sie den gewünschten Benutzernamen, die Domain und das Passwort in die entsprechenden Felder ein. Diese Option ist nur für Remote-Verbindungen verfügbar.

   Um eine störungsfreie Verbindung zwischen der Management-Konsole und dem Server herzustellen, verwenden Sie das Benutzerkonto Administrator, das standardmäßig in das auf dem Server installierte Betriebssystem integriert wurde, oder deaktiveren Sie die Benutzerkontensteuerung (UAC). Andernfalls werden das Programm-Monitoring und die Lizenzverwaltung nicht verfügbar sein.

4. Zum verbinden mit dem Server klicken Sie auf die Schaltfläche **Fertig**.

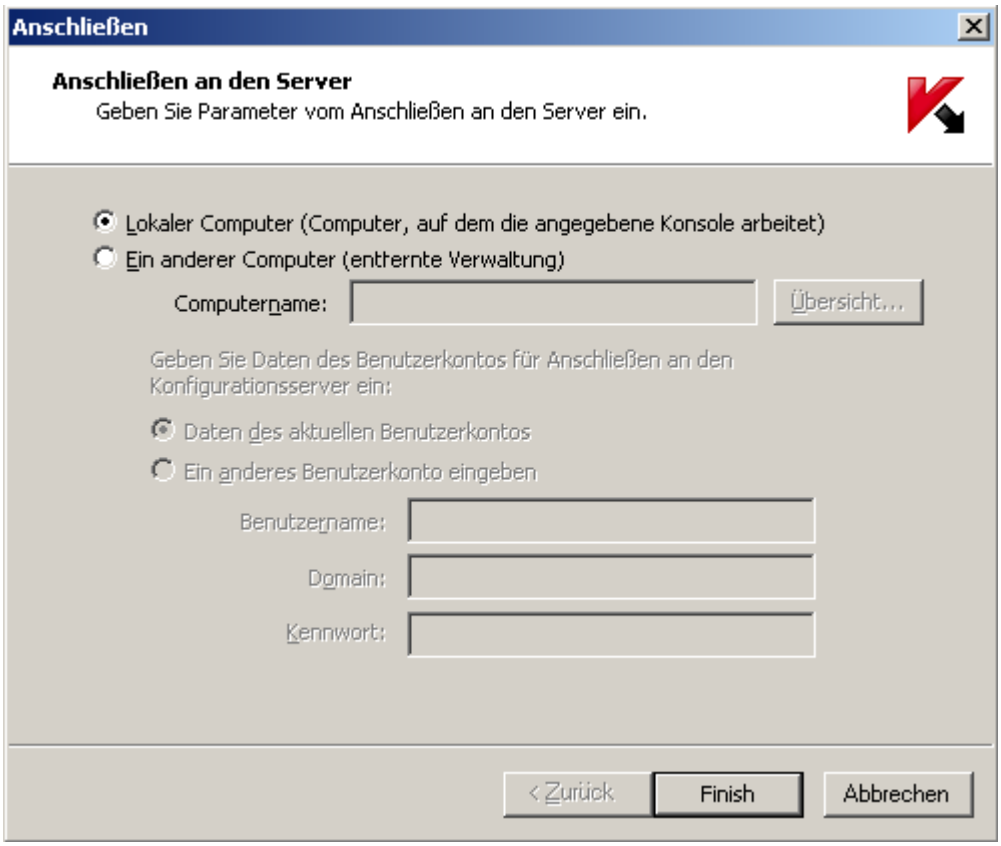

Abbildung 5. Fenster für die Serververbindung

ÜBERPRÜFUNG DER PROGRAMMEINSTELLUNGEN

Nach Installation und Anpassung von Kaspersky Security sollten Sie die Richtigkeit der gewählten Einstellungen und die ordnungsgemäße Funktion der Anwendung mithilfe des mitgelieferten "Testvirus" und seiner Modifikationen überprüfen.

Dieser "Testvirus" wurde vom Institut EICAR (The European Institute for Computer Anti-Virus Research) speziell zum Überprüfen der Arbeit von Virenschutzprogrammen entwickelt. Der "Testvirus" ist kein schädliches Programm und enthält keine Programmcodes, die auf Ihrem Computer Schaden anrichten können. Die Virenschutzprogramme der meisten Hersteller erkennen ihn jedoch als Virus.

Der "Testvirus" kann von der offiziellen Internetseite des EICAR-Instituts heruntergeladen werden: http://www.eicar.org/anti_virus_test_file.htm.

Diese Datei enthält den "Viren"körper des Standard-"Testvirus". Kaspersky Anti-Virus erkennt den "Testvirus", weist ihm den Status "Infiziert" zu und führt die vom Administrator für diesen Objekttyp festgelegte Aktion aus.

Um zu überprüfen, wie das Programm beim Auffinden anderer Objekttypen reagiert, können Sie den Standard-"Testvirus" modifizieren, indem Sie bestimmte Präfixe hinzufügen s. Tabelle unten). Zum Erstellen dieser modifizierten "Testviren" können Sie jedes beliebige Text- und Hypertextverarbeitungsprogramm verwenden.

Tabelle 1. Präfixe für den "Testvirus"

PRÄFIX	OBJEKTTYP
Kein Präfix, standardmäßiger "Testvirus"	Infiziert. Beim Desinfektionsversuch des Objekts tritt ein Fehler auf und die für irreparable Objekte geltende Aktion wird ausgeführt.
CORR-	Beschädigt.
SUSP-	Verdächtig (unbekannter Virencode).
WARN-	Verdächtig (Modifizierter bekannter Virencode).
ERRO-	Bei der Prüfung tritt der gleiche Fehler auf, wie beim Auffinden beschädigter Objekte.
CURE-	Infiziert (desinfizierbar). Das Objekt wird desinfiziert; dabei wird der Text im "Viren"körper ersetzt durch CURED.
DELE-	Infiziert (nicht desinfizierbar). Es werden die für nicht desinfizierbare Objekte festgelegten Aktionen ausgeführt.

Die erste Spalte der Tabelle enthält Präfixe, die dem standardmäßigen "Testvirus" am Zeilenanfang hinzugefügt werden können.

Speichern Sie nach dem Hinzufügen von Präfixen den "Testvirus" in einer Datei, z.B. mit dem Namen eicar_dele.com (so können Sie für jede Modifikation des "Virus" einen eindeutigen Namen vergeben).

In der zweiten Spalte werden die durch das Virenschutzprogramm nach Hinzufügen der Präfixe identifizierten Objekttypen beschrieben. Die auszuführenden Aktionen für jedes einzelne Objekt richten sich nach den vom Administrator festgelegten Parametern für die Virenprüfung.

IN DIESEM ABSCHNITT

Schutz für Datenströme über das HTTP-Protokoll überprüfen 31

Schutz für Datenströme über das FTP-Protokoll überprüfen 31

Schutz für Datenströme über das SMTP / POP3-Protokoll überprüfen 31

SCHUTZ FÜR DATENSTRÖME ÜBER DAS HTTP-PROTOKOLL ÜBERPRÜFEN

Um den Schutz für den Datenstrom über das HTTP-Protokoll zu überprüfen, gehen Sie folgendermaßen vor:

1. Öffnen Sie in Ihrem Browser den Link für den "Testvirus" http://www.eicar.org/download/eicar.com. Wenn Kaspersky Anti-Virus korrekt angepasst ist, wird der "Testvirus" nicht geladen und im Browser erscheint eine Meldung, dass der Link ein schädliches Objekt enthält.

2. Im Fenster **Monitoring** der Management-Konsole für Kaspersky Anti-Virus können Sie eine Statistik für die überprüften Objekte aufrufen: Der "Testvirus" sollte in der Spalte **HTTP** angezeigt werden. Überzeugen Sie sich davon, dass der "Testvirus" vom Programm gemäß den festgelegten Einstellungen im Fenster **Parameter der HTTP-Untersuchung** der der Management-Konsole verarbeitet wurde.

SCHUTZ FÜR DATENSTRÖME ÜBER DAS FTP-PROTOKOLL ÜBERPRÜFEN

Um den Schutz für den Datenstrom über das FTP-Protokoll zu überprüfen, gehen Sie folgendermaßen vor:

1. Versuchen Sie, die Datei mit dem "Testvirus" über einen beliebigen FTP-Client herunterzuladen. Wenn Kaspersky Anti-Virus korrekt angepasst ist, wird der "Testvirus" gesperrt.

2. Im Fenster **Monitoring** der Management-Konsole für Kaspersky Anti-Virus können Sie eine Statistik für die überprüften Objekte aufrufen: der "Testvirus" sollte in der Spalte **FTP** angezeigt werden.

SCHUTZ FÜR DATENSTRÖME ÜBER DAS SMTP / POP3-PROTOKOLL ÜBERPRÜFEN

Um den Schutz für Datenströme über das SMTP-Protokoll zu überprüfen, müssen Sie eine E-Mail mit dem "Testvirus" im Anhang mit einem E-Mail-Programm versenden, welches das SMTP-Protokoll verwendet. Der "Testvirus" wird entsprechend den im Fenster **Parameter der SMTP-Untersuchung** der Management-Konsole für Kaspersky Anti-Virus gewählten Einstellungen ersetzt. Im Fenster **Monitoring** der Management-Konsole können Sie eine Statistik für die überprüften Objekte aufrufen: Der "Testvirus" sollte in der Spalte **SMTP / POP3** angezeigt werden.

Um den Schutz für Datenströme über das POP3-Protokoll zu überprüfen, müssen Sie eine E-Mail mit dem "Testvirus" im Anhang mit einem E-Mail-Programm versenden, welches das POP3-Protokoll verwendet. Hierzu können Sie beispielsweise eine E-Mail mit dem "Testvirus" an ihre eigene E-Mail-Adresse versenden, nachdem Sie zuvor die Überwachung für den E-Mail-Verkehr über SMTP deaktiviert haben. Der "Testvirus" wird entsprechend den im Fenster **Parameter der POP3-Untersuchung** der Management-Konsole für Kaspersky Anti-Virus gewählten Einstellungen ersetzt. Im Fenster **Monitoring** der Management-Konsole können Sie eine Statistik für die überprüften Objekte aufrufen: Der "Testvirus" sollte in der Spalte **SMTP / POP3** angezeigt werden.

GRUNDEINSTELLUNGEN FÜR DEN DATENSTROM-SCHUTZ

Nach der Installation verwendet Kaspersky Anti-Virus die standardmäßigen Grundeinstellungen für den Schutz des Datenstroms der angeschlossenen Client-Computer. Überwacht wird der Datenstrom über das HTTP-, FTP-, POP3- und SMTP-Protokoll. Gefundene schädliche und verdächtige Objekte werden durch Kaspersky Anti-Virus gesperrt und die entsprechenden Objekte durch eine Standardmeldung über gefundene Bedrohungen ersetzt.

Die Richtlinien für die Virenprüfung gelten für alle Computer.

SIEHE AUßERDEM:

Virenprüfung..... 39

Richtlinien für die Virenprüfung pflegen 44

DATENBANKUPDATES

Jeden Tag tauchen neue Viren, trojanische Programme und andere Malware auf. Für einen zuverlässigen Schutz des Datenstroms werden stets aktuelle Informationen zu Bedrohungen und Möglichkeiten für deren Bekämpfung benötigt. Diese Daten sind in den Anti-Viren-Datenbanken gespeichert, die das Programm für den Anti-Virenschutz verwendet. Um stets den bestmöglichen Anti-Virenschutz zu gewährleisten müssen die Datenbanken laufend aktualisiert werden.

Es wird empfohlen, sofort nach Installation des Programms ein Datenbankupdate auszuführen, da die im Installationspaket enthaltenen Datenbanken zum Zeitpunkte der Installation sicher veraltet sein werden.

Auf den Updateservern von Kaspersky Lab werden die Anti-Viren-Datenbanken regelmäßig einmal pro Stunde aktualisiert. Wir empfehlen, in den Einstellungen eine automatische Aktualisierung der Datenbanken mit diesem Zeitintervall vorzusehen (s. Abschnitt "Datenbanken automatisch aktualisieren" ab S. 34).

Für das Update der Anti-Viren-Datenbanken stehen folgende Quellen zur Verfügung:

- Updateserver von Kaspersky Lab im Internet (s. Abschnitt "Einstellungen für Datenbankupdates über Internet anpassen" ab S. 36);
- lokale Updatequellen: lokale oder Netzwerkordner (s. Abschnitt "Updatequelle für Datenbanken auswählen" ab S. 35).

Während des Updates werden die auf dem Computer installierten Datenbanken mit den Datenbanken der Updatequelle abgeglichen. Wenn diese sich voneinander unterscheiden, werden die fehlenden Updates zusätzlich installiert. Datenbanken und Module werden nicht vollständig kopiert, wodurch die Updategeschwindigkeit wesentlich gesteigert und der Netzwerkverkehr entlastet wird.

Datenbanken können automatisch nach einem festgelegten Zeitplan oder manuell aktualisiert werden. Nach dem Kopieren der Dateien von der ausgewählten Updatequelle aktiviert das Programm automatisch die neuen Datenbanken und setzt die Datenstrom-Prüfung mit diesen fort.

Sie können jederzeit die ordnungsgemäße Funktion für automatische Updates prüfen und Statusinformationen zu Datenbanken abrufen (s. Abschnitt "Statusinformationen zu Datenbanken abrufen" ab S. 33).

IN DIESEM ABSCHNITT

Statusinformationen zu Datenbanken abrufen 33

Manuelles Update der Datenbanken 34

Automatisches Update der Datenbanken 34

Updatequelle für Datenbanken auswählen 35

Einstellungen für Datenbankupdates über Internet anpassen 36

Datenbankupdate aus einem Netzwerkordner 37

STATUSINFORMATIONEN ZU DATENBANKEN ABRUFEN

Um Statusinformationen zu den verwendeten Datenbanken abzurufen gehen Sie folgendermaßen vor:

1. Markieren Sie in der Konsolenstruktur den Knoten für den gewünschten Server.
2. Klicken Sie auf die Schaltfläche **Virenprüfung**. Es erscheint das Fenster **Virenprüfung** in der Registerkarte **Update**.

Informationen zu den verwendeten Datenbanken werden Ihnen im Feld **Informationen zu den verwendeten Datenbanken** angezeigt. Hier können Sie Erstellungsdatum und -uhrzeit sowie die Anzahl der Einträge für die Datenbanken ablesen.

MANUELLES UPDATE DER DATENBANKEN

Verwenden Sie das manuelle Update, wenn die vorhandenen Datenbanken sofort aktualisiert werden sollen.

Um die Datenbanken für Kaspersky Anti-Virus manuell zu aktualisieren, gehen Sie folgendermaßen vor:

1. Markieren Sie in der Konsolenstruktur den Knoten für den gewünschten Server.
2. Klicken Sie auf die Schaltfläche **Virenprüfung**. Es erscheint das Fenster **Virenprüfung** in der Registerkarte **Update**.
3. Klicken Sie auf die Schaltfläche **Jetzt aktualisieren**. Das Datenbankupdate wird gestartet. Der aktuelle Ausführungsstatus wird Ihnen im Feld rechts neben der Schaltfläche angezeigt.

AUTOMATISCHES UPDATE DER DATENBANKEN

Auf den Updateservern von Kaspersky Lab werden die Anti-Viren-Datenbanken regelmäßig einmal pro Stunde aktualisiert. Wir empfehlen Ihnen, ein automatisches Update der Datenbanken mit dem gleichen Zeitintervall vorzusehen. Dieser Wert ist auch in den Grundeinstellungen standardmäßig voreingestellt.

Um das automatische Datenbankupdate anzupassen, gehen Sie folgendermaßen vor:

1. Markieren Sie in der Konsolenstruktur den Knoten für den gewünschten Server.
2. Klicken Sie auf die Schaltfläche **Virenprüfung**. Es erscheint das Fenster **Virenprüfung** in der Registerkarte **Update**.
3. Überzeugen Sie sich, dass das Kontrollkästchen **Datenbanken automatisch aktualisieren** aktiviert ist (ist das Kontrollkästchen deaktiviert, erfolgen keine automatischen Updates für Datenbanken).
4. Wählen Sie eine der folgenden Varianten für das Zeitintervall zwischen zwei Updates:
   - **Jeden N-ten Tag um T1 und T2**: hierbei ist N – der Abstand zwischen zwei regelmäßigen Updates in Tagen, und T1 und T2 – die Uhrzeit, zu der Updates ausgeführt werden sollen. Wählen Sie z.B. N = 3, T1 = 23:15, T2 = 05:00, werden die Datenbanken am selben Tage zur festgelegten Uhrzeit zweimal aktualisiert, im Weiteren dann aller drei Tage. Der Einstellungen T2 ist nicht unbedingt erforderlich. Sie können ihn deaktivieren, indem Sie das entsprechende Häkchen entfernen.
   - **Einmal in T3**; T3 ist hierbei die Zeitspanne zwischen zwei aufeinander folgenden Updates. Wählen Sie z.B. T3 = 4 Stunden, so werden die Datenbanken regelmäßig im Abstand von vier Stunden aktualisiert.
5. Klicken Sie auf die Schaltfläche **Übernehmen**, um die Änderungen an den Parametern zu speichern, oder auf die Schaltfläche **OK**, um die Änderungen zu speichern und das Fenster zu schließen.
6. Wählen Sie eine Updatequelle aus (s. Abschnitt "Updatequelle für Datenbanken auswählen" ab S. 35).
7. Richten Sie die Einstellungen für das Update über Internet (s. Abschnitt "Einstellungen für das Update über Internet anpassen" ab S. 36) oder aus einem Netzwerkordner (s. Abschnitt "Datenbankupdate aus einem Netzwerkordner" ab S. 37) ein.

UPDATEQUELLE FÜR DATENBANKEN AUSWÄHLEN

Eine Updatequelle ist eine Ressource, die Updates der Datenbanken und der Module für Kaspersky Anti-Virus enthält. Standardmäßig erfolgt das Update aus dem Internet von den Kaspersky-Lab-Update-Servern. Dabei handelt es sich um spezielle Internetseiten, auf denen Updates der Datenbanken und Programm-Module für alle Kaspersky-Lab-Produkte zur Verfügung gestellt werden. Sie können festlegen, dass Updates von einem HTTP- bzw. FTP-Server oder aus einem lokalen bzw. Netzwerkordner geladen werden sollen. Das Programm verwendet die gewählte Updatequelle sowohl für automatische als auch manuelle Updates.

Um eine Updatequelle auszuwählen, gehen Sie folgendermaßen vor:

1. Markieren Sie in der Konsolenstruktur den Knoten für den gewünschten Server.

2. Klicken Sie auf die Schaltfläche **Virenprüfung**. Das Fenster **Virenprüfung** in der Registerkarte **Update** wird geöffnet (s. Abb. unten).

3. Wählen Sie in der Einstellungengruppe **Quelle** eine der folgenden Varianten:

   - **Kaspersky-Lab-Updateserver**: HTTP-, und FTP-Server von Kaspersky Lab im Internet, auf denen stündlich die neuesten Datenbankupdates zum Download bereitgestellt werden (diese Variante ist standardmäßig in den Grundeinstellungen vorgesehen);

   - **lokaler oder Netzwerkordner:** ein lokaler bzw. Netzwerkordner, in dem die per Internet heruntergeladenen Updates gespeichert werden. Falls Sie diese Variante wählen, geben Sie im Eingabefeld manuell oder über das Standardfenster des Microsoft-Windows-Explorers den Pfad für den Ordner ein. Um das Explorer-Fenster zu öffnen, klicken Sie auf die Schaltfläche **Auswahl**. Passen Sie nach Bedarf die weiteren Update-Parameter an (s. Abschnitt "Datenbankupdate aus einem Netzwerkordner" ab S. 37).

4. Klicken Sie auf die Schaltfläche **Übernehmen**, um die Änderungen an den Parametern zu speichern, oder auf die Schaltfläche **OK**, um die Änderungen zu speichern und das Fenster zu schließen.

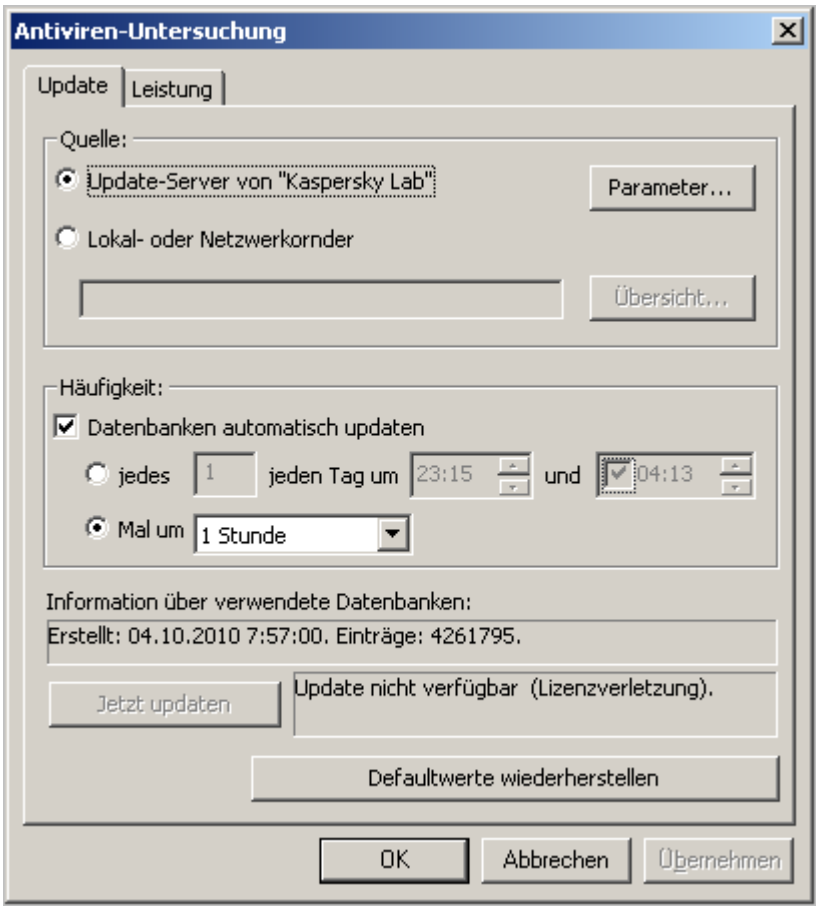

Abbildung 6. Registerkarte "Update"

EINSTELLUNGEN FÜR DATENBANKUPDATES ÜBER INTERNET ANPASSEN

Die gewählten Einstellungen werden sowohl für automatische als auch manuelle Updates der Anti-Viren-Datenbanken verwendet.

➧ *Um die Einstellungen für Updates über Internet zu ändern, gehen Sie folgendermaßen vor:*

1. Markieren Sie in der Konsolenstruktur den Knoten für den gewünschten Server.

2. Klicken Sie auf die Schaltfläche **Virenprüfung**. Es erscheint das Fenster **Virenprüfung** in der Registerkarte **Update**.

3. Klicken Sie auf die Schaltfläche **Parameter**, um das Fenster **Parameter vom Update durch Internet** zu öffnen.

4. Geben Sie die Einstellungen zur Auswahl des Kaspersky-Lab-Update-Servers ein:

   - **Update-Server automatisch auswählen**: wenn Sie diese Variante wählen, wird der geeignete Update-Server automatisch ausgewählt;

   - **Bestimmten Server verwenden**: wählen Sie diese Variante, wenn ein bestimmter Server verwendet werden soll, und geben Sie den Servernamen im entsprechenden Eingabefeld ein.

5. Passen Sie die Einstellungen für die Verwendung eines Proxyservers ein:

   - Falls die Internetverbindung über einen Proxyserver hergestellt wird, markieren Sie das Kästchen **Proxyserver verwenden**, und geben Sie folgende Verbindungseinstellungen ein: Adresse des Proxyservers und die Portnummer für die Verbindung;

   - Falls die Internetverbindung über den Proxyserver für Microsoft ISA Server / Forefront TMG des Servers hergestellt wird, auf dem auch Kaspersky Anti-Virus installiert ist, markieren Sie das Kästchen **Lokalen Proxyserver verwenden**;

   - Wenn für den Zugang über den Proxy-Server ein Passwort gebraucht wird, legen Sie die Authentifizierung für den Proxy-Benutzer fest. Markieren Sie hierzu das Kästchen **Authentifizierung verwenden**, und füllen Sie die Felder **Benutzername** und **Passwort** aus. Wenn auf dem Proxyserver die NTLM-Authentifizierung verwendet wird, muss der **Benutzername** die Domain im Format <Domain>\<Benutzername> enthalten. Wenn der Benutzer für den Proxyserver ein lokaler Benutzer, ist, müssen Sie die Eingabe des **Benutzernamens** in folgendem Format vornehmen: <Computername>\<Benutzername> oder \<Benutzername>.

6. Markieren Sie das Kästchen **Passiven FTP-Modus verwenden**, wenn zum Herstellen der Verbindung mit dem FTP-Update-Server der passive Modus verwendet werden soll.

7. Klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu speichern und das Fenster zu schließen.

DATENBANKUPDATE AUS EINEM NETZWERKORDNER

Methoden zur Freigabe-Verwaltung (Zuweisung von Rechten) des Netzwerkordners zur Ausführung von Update unterscheiden sich in Abhängigkeit vom Einrichtungsschema der Anwendung. Kaspersky Anti-Virus kann sowohl innerhalb einer Domain als auch innerhalb einer Arbeitsgruppe installiert werden.

IN DIESEM ABSCHNITT

Update aus einem Netzwerkordner: Kaspersky Anti-Virus innerhalb einer Domain 37

Update aus einem Netzwerkordner: Kaspersky Anti-Virus innerhalb einer Arbeitsgruppe 38

UPDATE AUS EINEM NETZWERKORDNER: KASPERSKY ANTI-VIRUS INNERHALB EINER DOMAIN

Jedem Computer innerhalb einer Domain ist ein eindeutiges Benutzerkonto zugeordnet, das denselben Namen hat, wie der Computer selbst. Für Prozesse, die auf einem Computer über das Benutzerkonto **System** gestartet werden, erfolgt beim Zugriff auf andere Computer die Autorisierung mit dem Benutzerkonto des Computers, auf dem die Prozesse gestartet wurden.

Um den Zugriff auf die Netzwerkressource zu gewähren, von der die Verteilung von Updates erfolgt, gehen Sie innerhalb der Domain folgendermaßen vor:

1. Vergeben Sie Netzwerkberechtigungen: vergeben Sie eine Leseberechtigung für diese Ressource für das Benutzerkonto des Computers in der Domain, auf dem Kaspersky Anti-Virus läuft.

2. Vergeben Sie lokale Zugriffrechte für dasselbe Benutzerkonto, für das Sie die Netzwerkberechtigungen vergeben haben.

   Die lokalen Zugriffsrechte müssen mindestens den gleichen Umfang haben, wie die zuvor vergebenen Netzwerkberechtigungen.

UPDATE AUS EINEM NETZWERKORDNER: KASPERSKY ANTI-VIRUS INNERHALB EINER ARBEITSGRUPPE

Die Daten für **System** für Computer, die zu einer Arbeitsgruppe zusammengefasst sind, können im Netzwerk nicht unterschieden werden. Sie können keine individuellen Berechtigungen für Prozesse vergeben, die vom Benutzerkonto **System** auf anderen Computern der Gruppe ausgeführt werden. Wenn Updates zentral für alle Computer einer Arbeitsgruppe erfolgen sollen, müssen Sie daher wie folgt vorgehen:

- Zugriffsberechtigungen für die Netzwerkressource an anonyme Nutzer vergeben (**ANONYMOUS LOGON**);
- spezielle Zugriffsrechte für die Netzwerkressource an anonyme Nutzer vergeben.

Nachfolgend wird die Zuordnung der Zugriffsberechtigungen erläutert.

Netzwerkberechtigungen vergeben

Die Leseberechtigung für die Netzwerkressource erhält das Benutzerkonto **ANONYMOUS LOGON**.

Lokale Zugriffsrechte vergeben

Die lokalen Zugriffsrechte werden für dieselben Benutzerkonten vergeben, wie die Netzwerkberechtigungen und müssen mindestens denselben Umfang haben, wie die Netzwerkberechtigungen.

Um Sonderrechte für den anonymen Zugriff auf die Netzwerkressource zu vergeben, führen Sie im Editor für die lokalen System-Sicherheitsrichtlinien von Microsoft Windows Server 2003 / 2008 folgende Schritte aus:

1. Starten Sie den Editor für lokale Richtlinien (**Start** → **Control Panel** → **Administrative Tools** → **Local Security Policy**).
2. Wählen Sie **Security Settings** → **Local Policies** → **Security Options**.
3. Wählen Sie im Ergebnisbereich **Network access: Shares that can be accessed anonymously**und öffnen Sie die Eigenschaften über das Kontextmenü. Geben Sie in der Registerkarte **Local PolicySetting** den Namen der Netzwerkressource ein, auf die der Zugriff erlaubt werden soll.
4. Um die geänderten Einstellungen zu übernehmen, wählen Sie im Kontextmenü des Knotens **Security Settings** den Punkt **Reload**.

VIRENPRÜFUNG

Um ein optimales Verhältnis von Performance und Sicherheit zu gewährleisten, können Sie die Einstellungen für die Virenprüfung nach Bedarf anpassen. Um die entsprechenden Einrichtungsfenster aufzurufen, wählen Sie in der Management-Konsole den Knoten für den gewünschten Server. Im Ergebnis fenster werden Ihnen nun die Schaltflächen zum Aufrufen der Einrichtungsfenster für die Einstellungen der Virenprüfung angezeigt.

IN DIESEM ABSCHNITT

Performanceeinstellungen für die Virenprüfung anpassen 39

Einstellungen für die Überwachung des Datenstroms über das HTTP-Protokoll anpassen 40

Einstellungen für die Überwachung des E-Mail-Verkehrs über FTP-Bericht anpassen 41

Einstellungen für die Überwachung des Datenstroms über SMTP-Protokoll anpassen 42

Einstellungen für die Überwachung des Datenstroms über POP3-Protokoll anpassen 43

PERFORMANCEEINSTELLUNGEN FÜR DIE VIRENPRÜFUNG ANPASSEN

Um das Fenster zum Anpassen der Performanceeinstellungen für die Virenprüfung aufzurufen, gehen Sie folgendermaßen vor:

1. Markieren Sie in der Konsolenstruktur den Knoten für den gewünschten Server.
2. Klicken Sie auf die Schaltfläche **Virenprüfung** in der Ergebnisleiste rechts.
3. Im folgenden Fenster klicken Sie auf die Registerkarte **Leistung**.

Als Grundeinstellungen sind folgende Werte für die Einstellungen vorgegeben:

- **Anzahl der Exemplare des Anti-Viren-Kernels**. Um die Verarbeitungsgeschwindigkeit für Kaspersky Anti-Virus bei der Verarbeitung großer Datenmengen zu steigern, werden mehrere Exemplare des Anti-Viren-Kernels gleichzeitig eingesetzt. Der Wert dieses Parameters wird standardmäßig als 2n+1 berechnet, wobei n der Anzahl der logischen Prozessoren von Microsoft ISA Server / Forefront TMG entspricht.
- **Davon nur zur Verarbeitung schneller Objekte** – 1. Der Anti-Viren-Kernel kann zu einem Zeitpunkt jeweils nur ein einzelnes Objekt verarbeiten. Um zu vermeiden, dass eventuell alle Kernels mit der Verarbeitung großer Objekte beschäftigt sind, während sich die kleineren Objekte aufstauen, empfehlen wir, mindesten eines der Anti-Viren-Kernel für die Verarbeitung "schneller" Objekte zu reservieren. Diese sogenannten "schnellen" Objekte sind ausschließlich HTTP-Objekte mit folgenden Einschränkungen:
  - Textobjekte mit einer Größe von weniger als 2 MB;
  - Grafikobjekte mit einer Größe von weniger als 2 MB;
  - alle sonstigen Objekte (ausgenommen ausführbare Dateien) mit einer Größe von weniger als256 KB.
- **Maximale Anzahl der im Speicher geprüften Objekte** – 128.
- **Maximale Größe der im Speicher geprüften Objekte** – 128 KB.

Die Filter von Kaspersky Anti-Virus können Objekte direkt zur Virenprüfung an den Anti-Viren-Kernel übertragen, ohne diese auf der Festplatte zu speichern. Bei Objekten, die größer sind, als der Vorgabewert für die Einstellungen **Maximale Größe der im Speicher geprüften Objekte**, oder falls die Anzahl der zur Überprüfung im Speicher geladenen Objekte den Vorgabewert für die **Maximale Anzahl der im Speicher geprüften Objekte** erreicht, werden die Objekte zuerst auf der Festplatte gespeichert.

- **Maximale Größe der Objektqueues für die Überprüfung** – 1024. Erreicht die Anzahl der Objekte in der Warteschlange den vorgegebenen Höchstwert, und es kommen weitere Objekte hinzu, so werden diese ohne Virenprüfung an die Client-Computer übertragen. Im Virenjournal des Programms erfolgt in diesem Fall ein entsprechender Eintrag, dass Objekte ohne Überprüfung weitergeleitet wurden (s. Abschnitt "Diagnose"66 ab S.).

- **Maximale Dauer der Prüfung** – 1800 s. Dauert die Virenprüfung länger, als der vorgegebene Maximalwert, wird das betreffende Objekt ohne Virenprüfung an die Client-Computer übertragen. Im Virenjournal des Programms erfolgt in diesem Fall ein entsprechender Eintrag, dass Objekte ohne Überprüfung weitergeleitet wurden (s. Abschnitt "Diagnose" ab S. 66).

- **Keine Objektcontainer prüfen mit einem Verschachtelungsgrad von** – 32 und höher. Maximal zulässiger Verschachtelungsgrad – 128.

Sie können diese Einstellungen ändern, um die Performance zu optimieren. Sämtliche bis hierher beschriebenen Einstellungen gelten für die Prüfung aller überwachten Protokolle. Um erneut die Grundeinstellungen zu verwenden, klicken Sie auf die Schaltfläche **Standardwerte wiederherstellen**.

Bei Verwendung von Download-Managern im Multithread-Download-Modus ist die Erhöhung des Datenverkehrs der Internet-Verbindung möglich. In diesem Fall steigert sich auch die Wahrscheinlichkeit, dass der Client ein schadhaftes, nicht untersuchtes Objekt empfängt. Dies ist mit den technischen Besonderheiten der Funktionsmechanismen von Download-Managern und Kaspersky Anti-Virus verbunden. Um das Risiko zu minimieren, wird es empfohlen, den Download-Manager im Multithread-Download-Modus nicht zu verwenden.

EINSTELLUNGEN FÜR DIE ÜBERWACHUNG DES DATENSTROMS ÜBER DAS HTTP-PROTOKOLL ANPASSEN

➧ *Um das Fenster zum Anpassen der Einstellungen aufzurufen, wählen Sie in der Konsolenstruktur den Knoten für den gewünschten Server,*

und klicken Sie auf die Schaltfläche **Parameter der HTTP-Untersuchung**, in der Ergebnisleiste rechts.

Als Grundeinstellungen sind folgende Werte für die Einstellungen vorgegeben:

- **Maximale Wartezeit bis zum Start der Datenübertragung an Client-Computer** – 30 S. Wenn nach dem Start des Downloads für ein Objekt mehr Zeit verstrichen ist, als der hier vorgegebene Höchstwert, und ein Objekt konnte immer noch nicht vollständig heruntergeladen oder nach dem Herunterladen überprüft werden, wird die Übertragung des Objekts an den Client-Computer schon vor Abschluss der Virenprüfung gestartet. Vollständig an Client-Computer übertragen werden jedoch nur überprüfte Objekte (sofern Sie keine Bedrohungen enthalten).

- **Nicht vor Abschluss der Prüfung an die Client-Computer übertragene Datenmenge** – 30%. Kaspersky Anti-Virus überprüft nur vollständig geladene Objekte. Um die Übertragung von Objekten an die Empfänger-Client-Computer zu beschleunigen, beginnt die Datenübertragung noch vor Abschluss der Prüfung. Es werden jedoch nur überprüfte Objekte vollständig übertragen (sofern sie keine Bedrohungen enthalten). Dieser Wert bestimmt den prozentualen Anteil der Datenmenge, die bis zum Abschluss der Prüfung zurückgehalten werden soll.

- **Geschwindigkeit zur Übertragung nicht geprüfter Objekte an Client-Computer**. Dieser Wert bestimmt, mit welcher Geschwindigkeit nicht überprüfte Objekte per HTTP-Bericht an Client-Computer übertragen werden. Den optimalen Wert für diesen Einstellungen können Sie nur durch praktische Erfahrung ermitteln, da dieser von der Geschwindigkeit der Virenprüfung und auch von der Kommunikationsgeschwindigkeit ihrer Hardware abhängt.

In diesem Fenster können Sie auch die Ersatz-Templates für gesperrte Dateien bearbeiten.

Um Ersatz-Templates für gesperrte Dateien zu bearbeiten, gehen Sie folgendermaßen vor.

1. Öffnen Sie das Fenster **Parameter der HTTP-Untersuchung**.
2. Klicken Sie auf die Schaltfläche **Ersatz-Template**.
3. Wählen Sie in dem folgenden Fenster den gesperrten Dateityp aus:
   - Infizierte Objekte.
   - Verdächtige Objekte.
   - Passwortgeschützte Objekte.
4. Klicken Sie auf die Schaltfläche **Ersatz-Template** neben dem entsprechenden Dateityp.

Die Templates werden im Format HTML gespeichert. Um die Templates zu bearbeiten, können Sie Standard-HTML-Tags verwenden. Möglicherweise in Templates enthaltene Makros:

- **%URL%**: Variable, die einen Link zu einem gefundenen gesperrten Objekt enthält;
- **%VIRUSNAME%**: Variable, die den Namen eines Virus enthält. Alle verfügbaren Makros können Sie über die Schaltfläche **Makros** anzeigen lassen.
- **%AV_SERVER%**: Name des Servers, auf dem Kaspersky Anti-Virus installiert ist.

Um wieder die Grundeinstellungen zu verwenden, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Fenster **Parameter der HTTP-Untersuchung**.
2. Klicken Sie auf die Schaltfläche **Standardwerte wiederherstellen**.

Durch Klick auf die Schaltfläche **Standardwerte wiederherstellen** werden sämtliche in den Grundeinstellungen vorgegebenen Einstellungenwerte und Ersatz-Templates wiederhergestellt.

EINSTELLUNGEN FÜR DIE ÜBERWACHUNG DES E-MAIL-VERKEHRS ÜBER FTP-BERICHT ANPASSEN

Um das Fenster zum Anpassen der Einstellungen aufzurufen, gehen Sie folgendermaßen vor:

1. Markieren Sie in der Konsolenstruktur den Knoten für den gewünschten Server.
2. Klicken Sie auf die Schaltfläche **Parameter der FTP-Untersuchung** in der Ergebnisleiste rechts.

Als Grundeinstellungen sind folgende Werte für die Einstellungen vorgegeben:

- **Maximale Zeitdauer für Prüfung des ersten Datenpakets**– 15 s. Wenn nach Empfang des ersten Datenpaketes mehr Zeit verstrichen ist, als der hier vorgegebene Höchstwert, und ein Objekt konnte immer noch nicht vollständig heruntergeladen oder nach dem Herunterladen überprüft werden, wird das Objekt ohne Virenprüfung an die Client-Computer übertragen.
- **Nicht vor Abschluss der Prüfung an die Client-Computer übertragene Datenmenge** – 10%. Kaspersky Anti-Virus überprüft nur vollständig geladene Objekte. Um die Übertragung von Objekten an die Empfänger-Client-Computer zu beschleunigen, beginnt die Datenübertragung noch vor Abschluss der Prüfung. Es werden jedoch nur überprüfte Objekte vollständig übertragen (sofern sie keine Bedrohungen enthalten). Dieser Wert

bestimmt den prozentualen Anteil der Datenmenge, die bis zum Abschluss der Prüfung zurückgehalten werden soll.

Um wieder die Grundeinstellungen zu verwenden, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Fenster **Parameter der FTP-Untersuchung**.
2. Klicken Sie auf die Schaltfläche **Standardwerte wiederherstellen**.

EINSTELLUNGEN FÜR DIE ÜBERWACHUNG DES DATENSTROMS ÜBER SMTP-PROTOKOLL ANPASSEN

Um das Fenster zum Anpassen der Einstellungen aufzurufen, gehen Sie folgendermaßen vor:

1. Markieren Sie in der Konsolenstruktur den Knoten für den gewünschten Server.
2. Klicken Sie auf die Schaltfläche **Parameter der SMTP-Untersuchung** in der Ergebnisleiste rechts.

   In den Grundeinstellungen sind folgende Einstellungswerte vorgegeben: **Betreffzeile für infizierte E-Mails ändern** – aktiviert.

Um das Ersatz-Template für die E-Mail-Betreffzeile zu bearbeiten,

klicken Sie auf die Schaltfläche **Ersatz-Template**.

Um Ersatz-Templates für gesperrte Dateien in demselben Fenster zu bearbeiten, gehen Sie folgendermaßen vor:

1. klicken Sie auf die Schaltfläche **Ersatz-Templates**.
2. Wählen Sie in dem folgenden Fenster den gesperrten Dateityp aus:
   - Infizierte Objekte.
   - Verdächtige Objekte.
   - Passwortgeschützte Objekte.
3. Klicken Sie auf die Schaltfläche **Ersatz-Template** für den gewählten Dateityp.

Die Templates werden im Format HTML gespeichert. Um die Templates zu bearbeiten, können Sie Standard-HTML-Tags verwenden. Möglicherweise in Templates enthaltene Makros:

- **%VIRUSNAME%**: Variable, die den Namen eines Virus enthält.

Alle verfügbaren Makros können Sie über die Schaltfläche **Makros** anzeigen lassen.

Um wieder die Grundeinstellungen zu verwenden, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Fenster **Parameter der SMTP-Untersuchung**.
2. Klicken Sie auf die Schaltfläche **Standardwerte wiederherstellen**.

Durch Klick auf die Schaltfläche **Standardwerte wiederherstellen** werden sämtliche in den Grundeinstellungen vorgegebenen Einstellungenwerte und Ersatz-Templates wiederhergestellt.

EINSTELLUNGEN FÜR DIE ÜBERWACHUNG DES DATENSTROMS ÜBER POP3-PROTOKOLL ANPASSEN

Um das Fenster zum Anpassen der Einstellungen aufzurufen, gehen Sie folgendermaßen vor:

1. Markieren Sie in der Konsolenstruktur den Knoten für den gewünschten Server.
2. Klicken Sie auf die Schaltfläche **Parameter der POP3-Untersuchung** in der Ergebnisleiste rechts.

Die Einstellungen für die Überwachung des Datenstroms über das POP3-Bericht sind die gleichen wie für die SMTP-Überwachung (s. Abschnitt "Einstellungen für die Überwachung des Datenstroms über das SMTP-Protokoll anpassen" ab S. 42).

RICHTLINIEN FÜR DIE VIRENPRÜFUNG PFLEGEN

Durch Richtlinien für die Virenprüfung können Sie verschiedene Regeln für die Verarbeitung von Berichten, Ausnahmen von der Virenprüfung und Aktionen beim Auffinden von Bedrohungen für unterschiedliche Netzwerkobjekte und Berichte vorgeben (s. Abschnitt "Netzwerkobjekte" ab S. 51). So können Sie beispielsweise vertrauenswürdige Absenderadressen für E-Mails definieren und bestimmte Dateitypen von der Virenprüfung ausschließen. Mithilfe von Richtlinien können Sie Untersuchungseinstellungen so definieren, dass ein optimales Verhältnis von Performance und Sicherheit gewährleistet ist.

Es werden drei Typen von Richtlinien unterschieden:

- **Richtlinien für die Verarbeitung von Berichten**: Einstellungen für die Verarbeitung des Datenstroms über FTP- und HTTP-Protokolle.
- **Richtlinien für Ausnahmen von der Prüfung**: Einstellungen zum Ausschließen von Objekten aus der Prüfung.
- **Richtlinien für die Virenprüfung**: Einstellungen für die Verarbeitung infizierter und passwortgeschützter Objekte.

Für jede Richtlinie sind bereits bestimmte Regeln in den Grundeinstellungen hinterlegt, die nicht geändert oder gelöscht werden können. Alle neu hinzugefügten Regeln erhalten eine höhere Priorität, als die in den Grundeinstellungen hinterlegten Regeln.

Die Anwendung der in Richtlinien definierten Regeln sieht in der Praxis folgendermaßen aus: Die Ausgangsdaten (Protokoll, Adresse des Netzwerkcomputers und Serveradresse) werden genutzt, um die prioritätsbasierende Regelliste zu überprüfen, bis die Anwendung ein zutreffendes Protokoll, eine Gruppe von Client-Adressen oder Gruppe von Servern findet, zu welchen die existierende Client-Adresse passt. Die gefundene Regel wird angewendet. Die oben beschriebene Prozedur wird für alle Regeln aller Richtlinientypen wiederholt.

Um eine Liste der vorhandenen Richtlinien und Regeln anzuzeigen, klicken Sie auf den Knoten **Richtlinien** (s. Abb. unten).

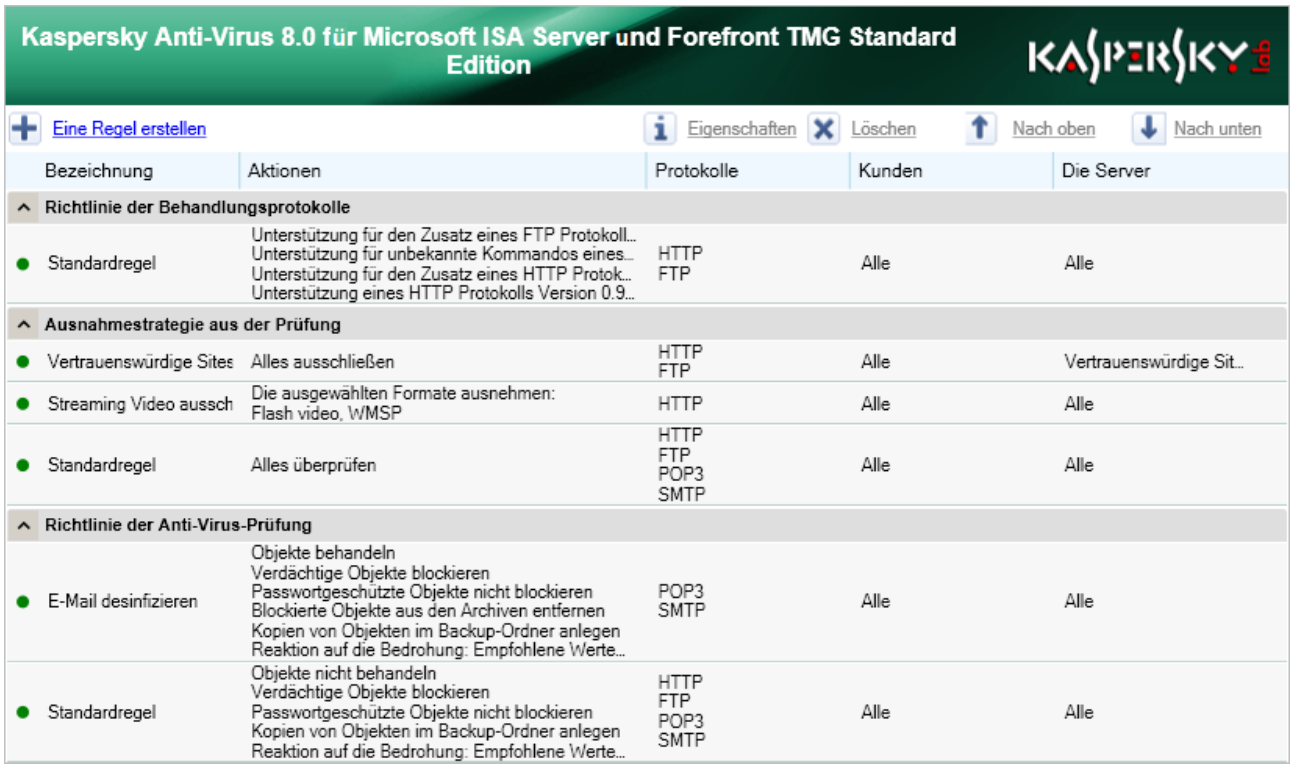

Abbildung 7. Fenster "Richtlinien"

IN DIESEM ABSCHNITT

Richtlinien für die Verarbeitung von Protokollen 45

Richtlinien für Ausnahmen von der Prüfung 46

Richtlinien für die Virenprüfung 46

Regeln zu Richtlinien hinzufügen 46

Priorität für Regeln in Richtlinien ändern 49

Einstellungen für Regeln in Richtlinien ändern 49

Regeln in Richtlinien deaktivieren 49

Regeln in Richtlinien löschen 50

RICHTLINIEN FÜR DIE VERARBEITUNG VON PROTOKOLLEN

Durch Richtlinien für die Verarbeitung von Berichten werden Einstellungen zur Verarbeitung des Datenstroms über das FTP- und HTTP-Protokoll für ausgewählte Objekte definiert.

Bei Verwendung der Grundeinstellungen wird für alle Computer die Regel **Default rule** angewendet.

Diese Regel besitzt für das FTP-Protokoll folgende Einstellungen:

- Wiederaufnahme von Downloads nach Unterbrechung wird nicht unterstützt;
- unbekannte Befehle vom FTP-Client werden nicht unterstützt.

Diese Regel besitzt für das HTTP-Bericht folgende Einstellungen:

- Wiederaufnahme von Downloads nach Unterbrechung wird nicht unterstützt;
- HTTP Version 0.9 wird nicht unterstützt.

RICHTLINIEN FÜR AUSNAHMEN VON DER PRÜFUNG

Durch Richtlinien für Ausnahmen von der Prüfung werden Ausnahmen definiert, so dass ausgewählte Netzwerkobjekte und Berichte von der Prüfung ausgenommen werden.

In den Grundeinstellungen sind folgende Regeln hinterlegt, die für alle Computer und Berichte angewendet werden:

- **Exclude trusted sites**. Durch diese Regel werden Objekte von der Prüfung ausgenommen, die über gemäß den Grundeinstellungen vertrauenswürdige Websites empfangen werden (z.B. kaspersky.com, microsoft.com).
- **Exclude streaming video**. Durch diese Regel werden Streaming-Videos von der Prüfung ausgenommen.
- **Default rule**. Diese Regel besitzt folgende Einstellungen:
  - Alle Dateitypen prüfen;
  - Inhalte von Archiven prüfen.

RICHTLINIEN FÜR DIE VIRENPRÜFUNG

Durch Richtlinien für die Virenprüfung werden Einstellungen zur Verarbeitung schädlicher, verdächtiger und passwortgeschützter Objekte ausgewählte Netzwerkobjekte und Berichte definiert.

Bei Verwendung der Grundeinstellungen wird für alle Computer und Berichte die Regel **Default rule** angewendet. Diese Regel besitzt folgende Einstellungen:

- alle gefundenen schädlichen Dateien blockieren;
- passwortgeschützte Objekte passieren lassen;
- schädliche Objekte nicht desinfizieren;
- verdächtige Objekte sperren;
- infizierte Teile zusammengesetzter Objekte nicht löschen.

REGELN ZU RICHTLINIEN HINZUFÜGEN

Sie können zu allen Richtlinien Regeln hinzufügen.

Gehen Sie folgendermaßen vor, um eine neue Regel für die Verarbeitung von Berichten zu erstellen:

1. Markieren Sie in der Konsolenstruktur den Knoten für den gewünschten Server. Wählen Sie nun den Knoten **Richtlinien**.

2. Klicken Sie auf die Schaltfläche **Regel erstellen**.

3. Wählen Sie in dem erscheinenden Menü den Punkt **Regel für die Verarbeitung von Berichten**. Der Assistent zum Erstellen einer neuen Regel wird geöffnet.

4. Geben Sie in dem folgenden Fenster im vorgesehenen Feld einen **Namen für die Regel** ein. Namen für Regeln müssen eindeutig sein. Klicken Sie nach Eingabe des namens auf die Schaltfläche **Weiter**.

5. Passen Sie im nächsten Fenster die Einstellungen zur Verarbeitung des Datenstroms für die einzelnen Protokolle an:

   - **Wiederaufnahme von Downloads unterstützen**: markieren Sie dieses Kästchen, wenn die Wiederaufnahme von Downloads nach Unterbrechung möglich sein soll.

   - **Unbekannte Befehle unterstützen**: Markieren Sie dieses Kästchen, um die Unterstützung für unbekannte Befehle vom FTP-Client zu aktivieren.

   - **HTTP 0.9 unterstützen**: Markieren Sie dieses Kästchen, um die Unterstützung für HTTP Version 0.9 zu aktivieren.

6. Klicken Sie auf die Schaltfläche **Weiter**.

7. Legen Sie im nächsten Fenster durch Markieren der entsprechenden Kästchen die Berichte fest, für welche die Regel angewendet werden soll. Klicken Sie auf die Schaltfläche **Weiter**.

8. Legen Sie im nächsten Fenster die Netzwerkobjekte fest, für deren ausgehenden E-Mail-Verkehr die Regel angewendet werden soll. Verwenden Sie die Schaltfläche **Hinzufügen**, um Netzwerkobjekte hinzuzufügen. Klicken Sie auf die Schaltfläche **Weiter**. Legen Sie im nächsten Fenster die Netzwerkobjekte fest, für deren eingehenden Datenstrom die Regel angewendet werden soll. Verwenden Sie die Schaltfläche **Hinzufügen**, um Netzwerkobjekte hinzuzufügen. Die Regel wird nur für den E-Mail-Verkehr zwischen den ausgewählten Computern und Servern angewendet.

9. Klicken Sie auf die Schaltfläche **Beenden**, um das Erstellen der Regel abzuschließen, oder verwenden Sie die Schaltflächen **Zurück** und **Weiter**, um zwischen den einzelnen Schritten des Assistenten zu navigieren.

10. Klicken Sie auf die Schaltfläche **Übernehmen** im unteren Teil des Fensters, damit die vorgenommenen Änderungen an den Richtlinien für die Virenprüfung wirksam werden.

➧ *Gehen Sie folgendermaßen vor, um eine Ausnahmeregel vom Berichtsfenster aus zu erstellen:*

1. Markieren Sie in der Konsolenstruktur den Knoten für den gewünschten Server. Wählen Sie nun den Knoten **Richtlinien**.

2. Klicken Sie auf die Schaltfläche **Regel erstellen**.

3. Wählen Sie in dem erscheinenden Menü den Punkt **Regel für Ausnahmen von der Prüfung**. Der Assistent zum Erstellen einer neuen Regel wird geöffnet.

4. Geben Sie in dem folgenden Fenster im vorgesehenen Feld einen **Namen für die Regel** ein. Namen für Regeln müssen eindeutig sein. Klicken Sie nach Eingabe des namens auf die Schaltfläche **Weiter**.

5. Wählen Sie im nächsten Fenster aus dem Dropdown-Menü einen der folgenden Werte:

   - **Alle Objekte ausschließen**: Alle Objekte werden von der Prüfung ausgeschlossen.

   - **Ausgewählte Objekttypen ausschließen**: Nur die ausgewählten Dateitypen werden von der Prüfung ausgeschlossen. Um die gewünschten Dateitypen auszuwählen, markieren Sie das Kästchen neben dem entsprechenden Namen.

   - **Alle Objekte überprüfen**: Es werden keine Dateitypen von der Prüfung ausgeschlossen.

6. Die Regel zur Verarbeitung von Archiven legen Sie fest, indem Sie das Kästchen **Inhalte von Archiven prüfen** markieren oder unmarkiert lassen. Klicken Sie auf die Schaltfläche **Weiter**.

7. Legen Sie im nächsten Fenster durch Markieren der entsprechenden Kästchen die Berichte fest, für welche die Regel angewendet werden soll. Klicken Sie auf die Schaltfläche **Weiter**.

8. Legen Sie im nächsten Fenster die Netzwerkobjekte fest, für deren ausgehenden E-Mail-Verkehr die Regel angewendet werden soll. Verwenden Sie die Schaltfläche **Hinzufügen**, um Netzwerkobjekte hinzuzufügen. Klicken Sie auf die Schaltfläche **Weiter**. Legen Sie im nächsten Fenster die Netzwerkobjekte fest, für deren eingehenden Datenstrom die Regel angewendet werden soll. Verwenden Sie die Schaltfläche **Hinzufügen**, um Netzwerkobjekte hinzuzufügen. Die Regel wird nur für den E-Mail-Verkehr zwischen den ausgewählten Computern und Servern angewendet.

9. Klicken Sie auf die Schaltfläche **Beenden**, um das Erstellen der Regel abzuschließen, oder verwenden Sie die Schaltflächen **Zurück** und **Weiter**, um zwischen den einzelnen Schritten des Assistenten zu navigieren.

10. Klicken Sie auf die Schaltfläche **Übernehmen** im unteren Teil des Fensters, damit die vorgenommenen Änderungen an den Richtlinien für die Virenprüfung wirksam werden.

Gehen Sie folgendermaßen vor, um eine Ausnahmeregel vom Berichtsfenster aus zu erstellen:

1. Markieren Sie in der Konsolenstruktur den Knoten für den gewünschten Server. Wählen Sie nun den Knoten **Richtlinien**.

2. Klicken Sie auf die Schaltfläche **Regel erstellen**.

3. Wählen Sie in dem erscheinenden Menü den Punkt **Regel für Virenprüfung**. Der Assistent zum Erstellen einer neuen Regel wird geöffnet.

4. Geben Sie in dem folgenden Fenster im vorgesehenen Feld einen **Namen für die Regel** ein. Namen für Regeln müssen eindeutig sein. Klicken Sie nach Eingabe des namens auf die Schaltfläche **Weiter**.

5. Klicken Sie im nächsten Fenster auf die Schaltfläche **Ändern**, um die bedrohungstypen auszuwählen, die gesperrt werden sollen. Markieren Sie in dem folgenden Fenster die Kästchen für die gewählten Bedrohungstypen, und klicken Sie auf die Schaltfläche **OK**. Sie können auch erweiterte Einstellungen zur Verarbeitung von Objekten festlegen:

   - **Verdächtige Objekte sperren**: Markieren Sie dieses Kästchen, wenn verdächtige Objekte gesperrt werden sollen.

   - **Desinfektion für Objekte versuchen**: Markieren Sie das Kästchen, wenn Kaspersky Anti-Virus versuchen soll, schädliche Objekte zu desinfizieren.

   - **Löschen versuchen für infizierte Teile zusammengesetzter Objekte**: Markieren Sie dieses Kästchen, wenn Kaspersky Anti-Virus versuchen soll, infizierte Teile zusammengesetzter Objekte zu löschen. Dieses Kästchen wird nur angezeigt, wenn auch das Kästchen **Desinfektion für Objekte versuchen** markiert ist.

   - **Kopien der Objekte im Backup-Ordner aufbewahren**: Markieren Sie das Kästchen, wenn vor dem Sperren, Desinfizieren oder Löschen von Objekten eine Kopie im Backup-Ordner gespeichert werden soll.

6. Klicken Sie auf die Schaltfläche **Weiter**.

7. Legen Sie im nächsten Fenster die Einstellungen zur Verarbeitung passwortgeschützter Objekte fest:

   - **Passwortgeschützte Objekte nicht zulassen**: Markieren Sie dieses Kästchen, wenn passwortgeschützte Objekte gesperrt werden sollen.

   - **Kopien der Objekte im Backup-Ordner aufbewahren:** Markieren Sie das Kästchen, wenn gesperrte passwortgeschützte Objekte im Backup-Ordner gespeichert werden sollen. Dieses Kästchen ist nur verfügbar, wenn das Kästchen **Passwortgeschützte Objekte nicht zulassen** aktiviert wird.

8. Klicken Sie auf die Schaltfläche **Weiter**.

9. Legen Sie im nächsten Fenster durch Markieren der entsprechenden Kästchen die Berichte fest, für welche die Regel angewendet werden soll. Klicken Sie auf die Schaltfläche **Weiter**.

10. Legen Sie im nächsten Fenster die Netzwerkobjekte fest, für deren ausgehenden E-Mail-Verkehr die Regel angewendet werden soll. Verwenden Sie die Schaltfläche **Hinzufügen**, um Netzwerkobjekte hinzuzufügen. Klicken Sie auf die Schaltfläche **Weiter**. Legen Sie im nächsten Fenster die Netzwerkobjekte fest, für deren eingehenden Datenstrom die Regel angewendet werden soll. Verwenden Sie die Schaltfläche **Hinzufügen**, um Netzwerkobjekte hinzuzufügen. Die Regel wird nur für den E-Mail-Verkehr zwischen den ausgewählten Computern und Servern angewendet.

11. Klicken Sie auf die Schaltfläche **Beenden**, um das Erstellen der Regel abzuschließen, oder verwenden Sie die Schaltflächen **Zurück** und **Weiter**, um zwischen den einzelnen Schritten des Assistenten zu navigieren.

12. Klicken Sie auf die Schaltfläche **Übernehmen** im unteren Teil des Fensters, damit die vorgenommenen Änderungen an den Richtlinien für die Virenprüfung wirksam werden.

PRIORITÄT FÜR REGELN IN RICHTLINIEN ÄNDERN

Gehen Sie folgendermaßen vor, um die Priorität einer Richtlinie zu ändern:

1. Markieren Sie in der Konsolenstruktur den Knoten für den gewünschten Server. Wählen Sie nun den Knoten **Richtlinien**.

2. Markieren Sie die Regel in der Tabelle, und klicken Sie auf die Schaltflächen **Nach oben** bzw. **Nach unten**, um die Priorität der Regel herauf- oder herabzusetzen.

3. Klicken Sie auf die Schaltfläche **Übernehmen** im unteren Teil des Fensters, damit die vorgenommenen Änderungen an den Richtlinien für die Virenprüfung wirksam werden.

EINSTELLUNGEN FÜR REGELN IN RICHTLINIEN ÄNDERN

Gehen Sie folgendermaßen vor, um die Priorität einer Richtlinie zu ändern:

1. Markieren Sie in der Konsolenstruktur den Knoten für den gewünschten Server. Wählen Sie nun den Knoten **Richtlinien**.

2. Markieren Sie die Regel in der Tabelle, und klicken Sie auf die Schaltfläche **Eigenschaften**, um das Fenster mit den Eigenschaften der Regel aufzurufen. Alternativ können Sie dieses Fenster auch durch Doppelklick auf die Regel öffnen.

3. Bearbeiten Sie nun die Einstellungen der Regel.

4. Klicken Sie auf **OK**, um die vorgenommenen Änderungen zu speichern.

5. Klicken Sie auf die Schaltfläche **Übernehmen** im unteren Teil des Fensters, damit die vorgenommenen Änderungen an den Richtlinien für die Virenprüfung wirksam werden.

REGELN IN RICHTLINIEN DEAKTIVIEREN

Um eine Regel innerhalb einer Richtlinie zu deaktivieren, gehen Sie folgendermaßen vor:

1. Markieren Sie in der Konsolenstruktur den Knoten für den gewünschten Server. Wählen Sie nun den Knoten **Richtlinien**.

2. Markieren Sie die Regel in der Tabelle, und klicken Sie auf die Schaltfläche **Eigenschaften**.

3. Im nächsten Fenster entfernen Sie auf der Registerkarte **Allgemein** das Häkchen im Kontrollkästchen **Aktivieren** einschalten.

4. Klicken Sie auf **OK**, um die vorgenommenen Änderungen zu speichern.

5. Klicken Sie auf die Schaltfläche **Übernehmen** im unteren Teil des Fensters, damit die vorgenommenen Änderungen an den Richtlinien für die Virenprüfung wirksam werden.

Um eine Regel innerhalb einer Richtlinie zu deaktivieren, gehen Sie in umgekehrter Reihenfolge vor.

REGELN IN RICHTLINIEN LÖSCHEN

Um eine Regel aus einer Richtlinie zu löschen, gehen Sie folgendermaßen vor:

1. Markieren Sie in der Konsolenstruktur den Knoten für den gewünschten Server. Wählen Sie nun den Knoten **Richtlinien**.

2. Markieren Sie die Regel in der Tabelle, und klicken Sie auf die Schaltfläche **Löschen**.

3. Bestätigen Sie das Löschen der Regel in dem erscheinenden Dialogfenster.

4. Klicken Sie auf die Schaltfläche **Übernehmen** im unteren Teil des Fensters, damit die vorgenommenen Änderungen an den Richtlinien für die Virenprüfung wirksam werden.

NETZWERKOBJEKTE

Netzwerkobjekte werden im Rahmen von Richtlinien verwendet. Es werden vier Typen von Netzwerkobjekten unterschieden:

- **Computer**: IP-Adressen von Computern;
- **Subnetz**: Gruppe von Computern, die zu einem ausgewählten Subnetz gehören;
- **Adressbereich**: Gruppe von Computern, deren Adressen zum ausgewählten Bereich gehören;
- **Domainnamen**: ein oder mehrere Computer, deren Domainnamen mit den ausgewählten Domainnamen übereinstimmt.

Klicken Sie auf den Knoten "Netzwerkobjekte". um eine Tabelle mit Beschreibungen zu allen Netzwerkobjekten anzuzeigen (s. Abb. unten).

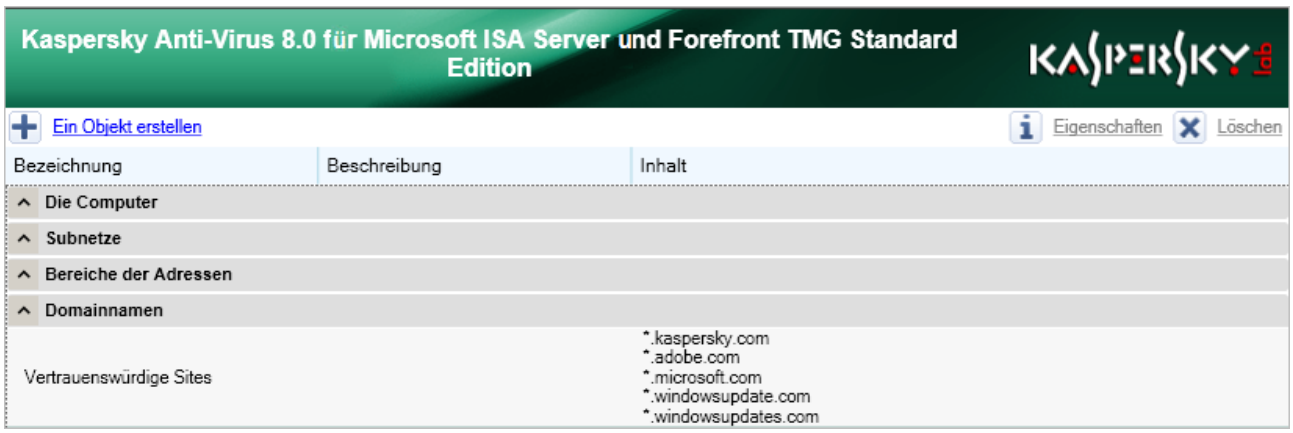

Abbildung 8. Fenster "Netzwerkobjekte"

IN DIESEM ABSCHNITT

Netzwerkobjekte erstellen 51

Einstellungen für Netzwerkobjekte ändern 53

Netzwerkobjekte löschen 53

NETZWERKOBJEKTE ERSTELLEN

Um Netzwerkobjekte vom Typ "Computer" zu erstellen, gehen Sie folgendermaßen vor:

1. Markieren Sie in der Konsolenstruktur den Knoten für den gewünschten Server. Wählen Sie nun den Knoten **Richtlinien** und anschließend **Netzwerkobjekte**.
2. Klicken Sie auf die Schaltfläche **Objekt erstellen**.
3. Wählen Sie in dem erscheinenden Menü den Punkt **Objekt "Computer" erstellen**.
4. Legen Sie im folgenden Fenster die Einstellungen für den Netzwerkadapter fest.

- **Name**: eindeutiger Name des Netzwerkobjekts;
- **IP**: IP-Adresse des Netzwerkobjekts;
- **Beschreibung**: detaillierte Beschreibung des Netzwerkobjekts.

5. Klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu speichern und das Fenster zu schließen.
6. Klicken Sie auf die Schaltfläche **Übernehmen** im unteren Teil des Fensters, damit die vorgenommenen Änderungen an Netzwerkobjekten wirksam werden.

Um Netzwerkobjekte vom Typ "Subnetz", zu erstellen, gehen Sie folgendermaßen vor:

1. Markieren Sie in der Konsolenstruktur den Knoten für den gewünschten Server. Wählen Sie nun den Knoten **Richtlinien** und anschließend **Netzwerkobjekte**.
2. Klicken Sie auf die Schaltfläche **Objekt erstellen**.
3. Wählen Sie in dem erscheinenden Menü den Punkt **Objekt "Subnetz" erstellen**.
4. Legen Sie im folgenden Fenster die Einstellungen für den Netzwerkadapter fest.
   - **Name**: eindeutiger Name des Netzwerkobjekts;
   - **IP**: IP-Adresse des Netzwerkobjekts;
   - **Maske**: Subnetzmaske;
   - **Beschreibung**: detaillierte Beschreibung des Netzwerkobjekts.
5. Klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu speichern und das Fenster zu schließen.
6. Klicken Sie auf die Schaltfläche **Übernehmen** im unteren Teil des Fensters, damit die vorgenommenen Änderungen an Netzwerkobjekten wirksam werden.

Um Netzwerkobjekte vom Typ "Adressbereich" zu erstellen, gehen Sie folgendermaßen vor:

1. Markieren Sie in der Konsolenstruktur den Knoten für den gewünschten Server. Wählen Sie nun den Knoten **Richtlinien** und anschließend **Netzwerkobjekte**.
2. Klicken Sie auf die Schaltfläche **Objekt erstellen**.
3. Wählen Sie in dem erscheinenden Menü den Punkt **Objekt "Adressbereich" erstellen**.
4. Legen Sie im folgenden Fenster die Einstellungen für den Netzwerkadapter fest.
   - **Name**: eindeutiger Name des Netzwerkobjekts;
   - **Anfangswert des Adressbereichs**: erste IP-Adresse des Bereichs;
   - **Endwert des Adressbereichs**: letzte IP-Adresse des Bereichs;
   - **Beschreibung**: detaillierte Beschreibung des Netzwerkobjekts.
5. Klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu speichern und das Fenster zu schließen.
6. Klicken Sie auf die Schaltfläche **Übernehmen** im unteren Teil des Fensters, damit die vorgenommenen Änderungen an Netzwerkobjekten wirksam werden.

Um Netzwerkobjekte vom Typ " "Domainnamen" zu erstellen, gehen Sie folgendermaßen vor:

1. Markieren Sie in der Konsolenstruktur den Knoten für den gewünschten Server. Wählen Sie nun den Knoten **Richtlinien** und anschließend **Netzwerkobjekte**.

2. Klicken Sie auf die Schaltfläche **Objekt erstellen**.

3. Wählen Sie in dem erscheinenden Menü den Punkt **Objekt "Domainnamen" erstellen**.

4. Legen Sie im folgenden Fenster die Einstellungen für den Netzwerkadapter fest.

   - **Name**: eindeutiger Name des Netzwerkobjekts;

   - **Beschreibung**: detaillierte Beschreibung des Netzwerkobjekts.

5. Klicken Sie auf die Schaltfläche **Hinzufügen**, und geben Sie in dem folgenden Fenster den Domainnamen ein, damit dieser zur Liste **Domains** hinzugefügt wird. Über die Schaltfläche **Löschen** können Sie Objekte aus der Liste entfernen. Der Domainname muss den Namen in der Standardform enthalten, z.B. microsoft.com oder msdn.microsoft.com. Der Domainname kann auch das Sonderzeichen ***** enthalten, das eine beliebige Anzahl Domains der untersten Ebene einschließt. So schließt z.B. der Domainname *****.microsoft.com die Domainnamen microsoft.com, www.microsoft.com, files.download.microsoft.com usw. ein. Das Zeichen ***** kann in einem Namen nur einmal verwendet werden. In Domainnamen können Sie keine Präfixe für Berichte (Templates der Form http://*.microsoft.com, ://microsoft.com usw.) eingeben; solche Templates werden als nicht korrekt erkannt und von Richtlinien ignoriert.

6. Klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu speichern und das Fenster zu schließen.

7. Klicken Sie auf die Schaltfläche **Übernehmen** im unteren Teil des Fensters, damit die vorgenommenen Änderungen an Netzwerkobjekten wirksam werden.

EINSTELLUNGEN FÜR NETZWERKOBJEKTE ÄNDERN

Um die Einstellungen für ein Netzwerkobjekt beliebigen Typs zu ändern, gehen Sie folgendermaßen vor:

1. Markieren Sie in der Konsolenstruktur den Knoten für den gewünschten Server. Wählen Sie nun den Knoten **Richtlinien** und anschließend **Netzwerkobjekte**.

2. Markieren Sie die Regel in der Tabelle, und klicken Sie auf die Schaltfläche **Eigenschaften**, um das Fenster mit den Eigenschaften des Objekts aufzurufen. Alternativ können Sie dieses Fenster auch durch Doppelklick auf das Objekt öffnen.

3. Bearbeiten Sie die Einstellungen des Netzwerkobjekts, und klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu speichern.

4. Klicken Sie auf die Schaltfläche **Übernehmen** im unteren Teil des Fensters, damit die vorgenommenen Änderungen an Netzwerkobjekten wirksam werden.

NETZWERKOBJEKTE LÖSCHEN

Um Netzwerkobjekte zu löschen, gehen Sie folgendermaßen vor:

1. Markieren Sie in der Konsolenstruktur den Knoten für den gewünschten Server. Wählen Sie nun den Knoten **Richtlinien** und anschließend **Netzwerkobjekte**.
2. Markieren Sie das Objekt in der Tabelle, und klicken Sie auf die Schaltfläche **Löschen**.
3. Bestätigen Sie das Löschen des Objekts in dem erscheinenden Dialogfenster.
   Das ausgewählte Objekt wird gelöscht.

Netzwerkobjekte können nur entfernt werden, wenn Sie nicht in benutzerdefinierte Richtlinien für die Virenprüfung eingebunden sind.

BERICHTE

In Kaspersky Anti-Virus können Sie für alle geschützten Berichte Ergebnisberichte zum Virenschutz für die angeschlossenen Client-Computer erstellen. Berichte sind Tabellen, in welchen Ereignisse und Aktionen während der Programmausführung aufgeführt werden.

Berichte können automatisch anhand eines voreingestellten Zeitplans oder auf Anforderung des Benutzers erstellt und auf Datenträgern gespeichert werden. Berichte werden im Format HTML im Unterordner **Reports** des Datenspeicherordners von Kaspersky Anti-Virus gespeichert. Sie können dann über den Internet Explorer angezeigt werden.

Aktionen für Berichte ausführen können Sie im gleichnamigen Fenster **Berichte** (s. Abb. unten). Hier können Sie Berichte erstellen, anzeigen und löschen sowie Einstellungen für Berichte anpassen. Einstellungen zum Erstellen von Berichten werden in speziellen Tasks zur Berichtserstellung festgelegt.

Um das Fenster **Berichte** aufzurufen, wählen Sie links in der Konsolenstruktur den Knoten für den gewünschten Server und anschließend den Knoten **Berichte**. Das Fenster **Berichte** erscheint rechts im Ergebnisbereich des Fensters. Im Fenster **Berichte** werden die vorhandenen Tasks zur Berichtserstellung als Liste angezeigt. Hier können Sie Tasks anzeigen, löschen und Taskeinstellungen anpassen. In der Liste werden folgende Daten angezeigt:

- **Taskname**: Name für Tasks zur Berichtserstellung.
- **Taskstatus**: aktueller Status für Tasks zur Berichtserstellung.
- **Ergebnis der Ausführung**: Ergebnis der letztmaligen Ausführung für Tasks zur Berichtserstellung.

Sie können bei bedarf neue Tasks hinzufügen. Für diese müssen Sie die Einstellungen Berichtszeitraum, Name, Beschreibung und Detaillierungsgrad festlegen.

Abbildung 9. Fenster "Berichte"

IN DIESEM ABSCHNITT

Tasks zur Berichtserstellung erstellen 55

Berichte anzeigen 55

Berichte löschen 56

Tasks für Berichtserstellung löschen 56

Eigenschaften für die Berichtserstellung ändern 56

Allgemeine Eigenschaften von Berichten ändern 56

Statistikdaten für Berichte löschen 57

TASKS ZUR BERICHTSERSTELLUNG ERSTELLEN

Um Tasks zur Berichtserstellung zu erstellen, gehen Sie folgendermaßen vor:

1. Wählen Sie in der Konsolenstruktur den Node für den gewünschten Server und anschließend den Node Berichte. **Berichte**. Das Fenster **Berichte** erscheint rechts im Ergebnisbereich des Fensters.

2. Klicken Sie auf **Hinzufügen**. Der Assistent für das Hinzufügen von Tasks zur Berichtserstellung wird geöffnet.

3. Geben Sie im ersten Fenster **Taskinformation** des Assistenten im Feld **Taskname** den Namen und im Feld **Beschreibung** eine Beschreibung für den Task ein. Klicken Sie auf die Schaltfläche **Weiter**.

4. Geben Sie im nächsten Fenster **Berichtseinstellungen** den gewünschten Detaillierungsgrad für den Bericht ein: **Standard** oder **Detailliert**. Wählen Sie den Zeitraum, für den der Bericht erstellt werden soll. Klicken Sie auf die Schaltfläche **Weiter**.

5. Im nächsten Fenster **Berichtseinstellungen** können Sie festlegen, dass der Bericht automatisch erstellt werden soll. Markieren Sie hierzu das Kästchen **Bericht automatisch erstellen**, und richten Sie einen Zeitplan für die Berichtserstellung ein. Wird das Kästchen nicht markiert, müssen Sie künftig die Berichtserstellung manuell anstoßen. Klicken Sie auf die Schaltfläche **Fertig stellen**.

   Sie haben nun einen neuen Task zur Berichtserstellung angelegt. Dieser wird mit den festgelegten Parametern in der Liste angezeigt. Wenn der Modus automatische Berichtserstellung gewählt wurde, wird der Bericht zum vorgegebenen Zeitpunkt erstellt. Wenn der Modus manuelle Berichtserstellung gewählt wurde, müssen Sie zum Starten auf die Schaltfläche **Bericht erstellen** klicken.

Der aktuelle Status für Tasks zur Berichtserstellung wird in der Spalte **Taskstatus** der Übersichtstabelle für Berichte angezeigt.

In Berichten werden keine auf Null zurückgesetzten Daten angezeigt, wenn ein Datum, zu dem die Statistik auf Null zurückgesetzt wurde, innerhalb des gewählten Berichtszeitraums liegt. Statistikdaten können manuell gelöscht werden. Sie werden automatisch gelöscht, wenn die festgelegte maximale Aufbewahrungsfrist erreicht wird (Grundeinstellung: 1 Jahr).

BERICHTE ANZEIGEN

Gehen Sie folgendermaßen vor, um einen Bericht anzuzeigen:

1. Wählen Sie in der Konsolenstruktur den Knoten für den gewünschten Server und anschließend den Knoten **Berichte**. Das Fenster **Berichte** erscheint rechts im Ergebnisbereich des Fensters.

2. Wählen Sie aus der Liste den Task zur Berichtserstellung aus, über den der gewünschte Bericht erstellt werden soll.

3. Klicken Sie auf die Schaltfläche **Bericht anzeigen**. Der zuletzt erstellte Bericht wird geöffnet. Eine Liste aller Berichte können Sie in der Registerkarte **Berichte** unter den Eigenschaften für Tasks zur Berichtserstellung aufrufen.

4. Wählen Sie Sie im folgenden Fenster den gewünschten Bericht aus, und klicken Sie auf die Schaltfläche **Anzeigen**. Der gewählte Bericht wird Ihnen in einem neuen Fenster angezeigt.

BERICHTE LÖSCHEN

Um einen vorhandenen Bericht zu löschen, gehen Sie folgendermaßen vor:

1. Wählen Sie in der Konsolenstruktur den Knoten für den gewünschten Server anschließend den Knoten **Berichte**. Das Fenster **Berichte** erscheint rechts im Ergebnisbereich des Fensters.

2. Öffnen Sie das Kontextmenü für den Task zur Berichtstellung, in der Sie einen Bericht löschen möchten, und wählen Sie den Punkt **Eigenschaften**. Das Fenster für die Taskeigenschaften wird geöffnet.

3. Im folgenden Fenster gehen Sie auf die Registerkarte **Berichte**.

4. Markieren Sie den gewünschten Bericht, und klicken Sie auf die Schaltfläche **Löschen**.

TASKS FÜR BERICHTSERSTELLUNG LÖSCHEN

Um Tasks zur Berichtserstellung zu löschen, gehen Sie folgendermaßen vor:

1. Wählen Sie in der Konsolenstruktur den Knoten für den gewünschten Server anschließend den Knoten **Berichte**. Das Fenster **Berichte** erscheint rechts im Ergebnisbereich des Fensters.

2. Öffnen Sie das Kontextmenü für den Task zur Berichtstellung, und wählen Sie den Punkt **Löschen**.

EIGENSCHAFTEN FÜR DIE BERICHTSERSTELLUNG ÄNDERN

Um Eigenschaften für Tasks zur Berichtserstellung zu ändern, gehen Sie folgendermaßen vor:

1. Wählen Sie in der Konsolenstruktur den Knoten für den gewünschten Server und anschließend den Knoten **Berichte**. Das Fenster **Berichte** erscheint rechts im Ergebnisbereich des Fensters.

2. Öffnen Sie das Kontextmenü für den Task zur Berichtstellung, und wählen Sie den Punkt **Eigenschaften**. Das Fenster für die Taskeigenschaften wird geöffnet.

3. Bearbeiten Sie die Taskeigenschaften (s. Abschnitt "Tasks für Berichtserstellung erstellen" ab S. 55).

ALLGEMEINE EIGENSCHAFTEN VON BERICHTEN ÄNDERN

Um allgemeine Eigenschaften für Berichte zu ändern, gehen Sie folgendermaßen vor:

1. Wählen Sie in der Konsolenstruktur den Knoten für den gewünschten Server und anschließend den Knoten **Berichte**. Öffnen Sie das Kontextmenü und gehen Sie auf den Punkt **Eigenschaften**. Das Fenster mit den allgemeinen Eigenschaften für Berichte wird geöffnet.

2. Im folgenden Fenster können Sie die Berichtserstellung aktivieren / deaktivieren, indem Sie das Kästchen **Aufzeichnen von Statistikdaten aktivieren** markieren bzw. die Markierung entfernen.

3. Um die Aufbewahrungsfrist für Berichte anzupassen, wählen Sie den gewünschten Zeitraum im Feld **Aufbewahrungsfrist**.

4. Um wieder die Grundeinstellungen zu verwenden, klicken Sie auf die Schaltfläche **Standardwerte wiederherstellen**.

STATISTIKDATEN FÜR BERICHTE LÖSCHEN

Die Statistikdaten, aus welchen Berichte erstellt werden, werden in einer separaten Datenbank gespeichert. Diese Daten werden automatisch gelöscht, sobald die in den allgemeinen Eigenschaften festgelegte Aufbewahrungsfrist (laut Grundeinstellungen 1 Jahr) erreicht ist. Enthält die Datenbank ein sehr großes Datenvolumen, kann dies die Verarbeitungsgeschwindigkeit beeinträchtigen. Bei Bedarf können Sie Statistikdaten auch manuell löschen.

Um Statistikdaten zu löschen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Fenster Allgemeine Eigenschaften für Berichte (s. Abschnitt "Allgemeine Eigenschaften für Berichte" ab S. 56).

2. Klicken Sie auf die Schaltfläche **Statistikdaten löschen**.

MONITORING DER PROGRAMMAUSFÜHRUNG

Im Fenster **Monitoring** (s. Abb. unten) können Sie jederzeit die ordnungsgemäße Ausführung von Kaspersky Anti-Virus kontrollieren, z.B. Funktionseinstellungen überprüfen und Statistiken zu überprüften Objekten anzeigen, sämtliche Filterfunktionen sowie den Status der Antiviren-Datenbanken und Ihrer Lizenz überprüfen.

Um das Fenster **Monitoring** aufzurufen, wählen Sie in der Konsolenstruktur den Knoten für den gewünschten Server und anschließend den Knoten **Monitoring**. Das Fenster **Monitoring** erscheint rechts im Ergebnisbereich des Fensters.

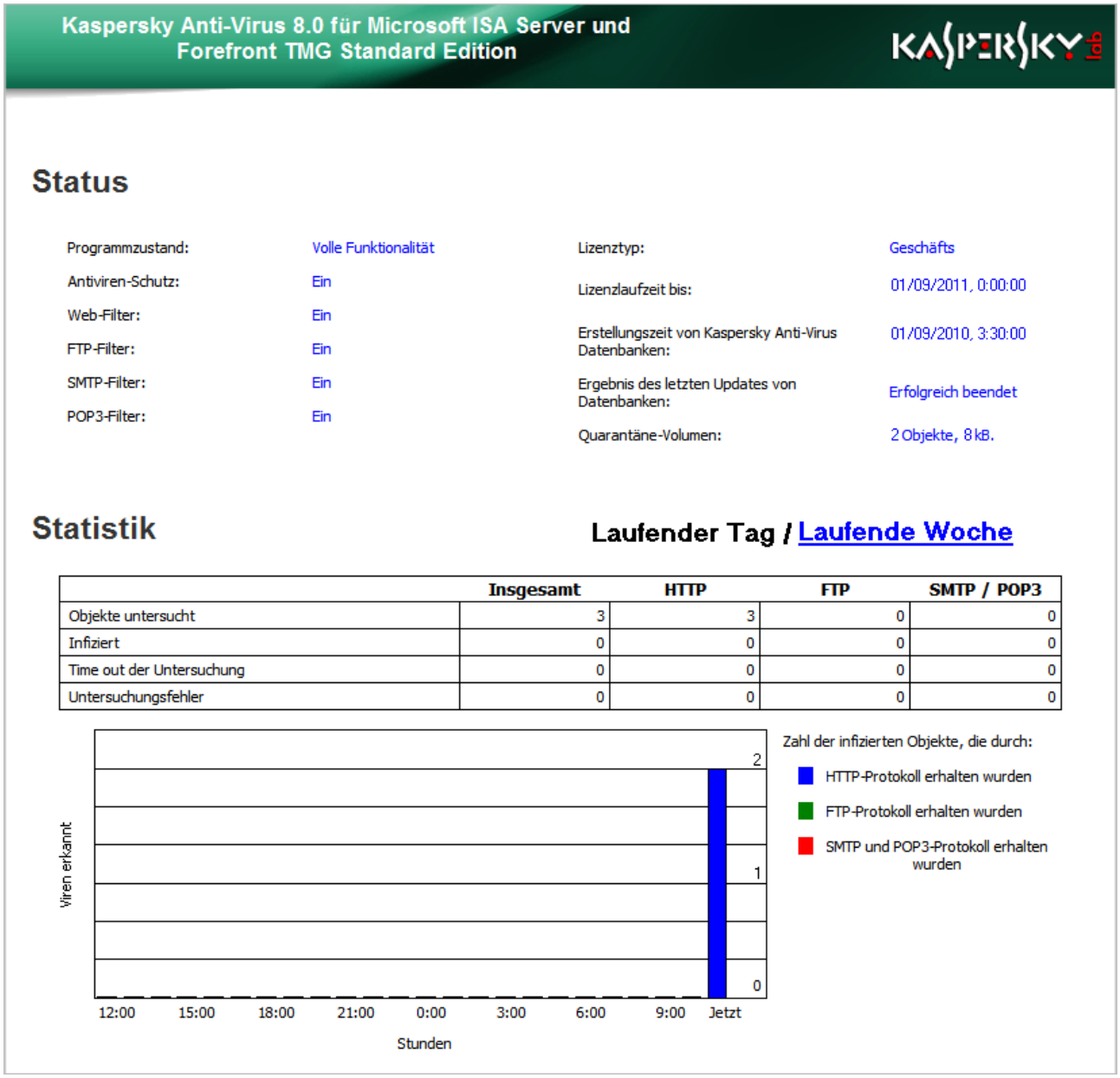

Abbildung 10. Fenster "Monitoring"

IN DIESEM ABSCHNITT

Ausführungsstatus von Kaspersky Anti-Virus 59

Statistik zur Ausführung von Kaspersky Anti-Virus 60

AUSFÜHRUNGSSTATUS VON KASPERSKY ANTI-VIRUS

In der leiste **Status** werden Ihnen folgende Informationen zu Funktionseinstellungen für Kaspersky Anti-Virus angezeigt:

- **Programmstatus**: Beschreibung der Programmfunktionen. Folgende Werte sind möglich:
  - Schutz ist aktiviert, Datenbankupdates nicht verfügbar;
  - Nur Datenbankupdates verfügbar;
  - Programm verfügbar, Datenbankupdates werden nicht ausgeführt;
  - Volle Funktionalität.
- **Virenschutz**: Ausführungsstatus für den Virenschutz. Ist der Virenschutz nicht aktiviert, wird der E-Mail-Verkehr der angeschlossenen Client-Computer nicht überwacht. Folgende Werte sind möglich:
  - Deaktiviert;
  - Aktiviert;
  - Interner Fehler. Schutz nicht verfügbar;
  - Eingeschränkt auf Grund der Lizenz.
- **Web-, FTP-, SMTP-, und POP3-Filter**: Ausführungsstatus für Filter (aktiviert / deaktiviert). Der Datenstrom für ein bestimmtes Protokoll ist nur dann vor Viren geschützt, wenn der entsprechende Programmfilter aktiviert ist.
- **Lizenztyp**: Typ der Lizenz. Es werden folgende Lizenztypen unterschieden:
  - Kommerzielle Lizenz: rechtmäßig erworbene Lizenz zur Aktivierung der Programme von Kaspersky Lab. Eine kommerzielle Lizenz ermöglicht die ordnungsgemäße Nutzung der Programme über die zum Verkaufszeitpunkt bestimmte Gültigkeitsdauer.
  - Probelizenz: Dient zum Kennenlernen der Programmfunktionen für Produkte von Kaspersky Lab für einen beschränkten Zeitraum. Probelizenzen werden von Kaspersky Lab kostenlos vergeben.

Wenn keine Lizenz installiert ist, erscheint im betreffenden Feld eine entsprechende Fehlermeldung.

- **Gültigkeitsdauer der Lizenz**: Datum, bis zu dem die aktuelle Lizenz gültig ist.
- **Erscheinungsdatum der Anti-Viren-Datenbanken**: Veröffentlichungsdatum und -zeit der verwendeten Anti-Viren-Datenbanken.
- **Ergebnis des letzten Updates** der Datenbanken: Ergebnis des letzten Updates der Anti-Viren-Datenbanken.
- **Größe des Backup-Ordners**: Gesamtzahl der Objekte im Backup-Ordner bzw. vom Backup-Ordner belegter Speicherplatz auf dem Datenträger (in Kilobyte).

STATISTIK ZUR AUSFÜHRUNG VON KASPERSKY ANTI-VIRUS

In der Leiste **Statistik** werden alle Statistikdaten zu geprüften Objekten angezeigt. Die Tabelle enthält Angaben zur Anzahl geprüfter und infizierter Objekte, Anzahl Timeouts bei der Prüfung von Objekten und Anzahl aufgetretener Fehler während der Virenprüfung. Alle Daten werden sowohl als Gesamtübersicht als auch gesplittet nach HTTP-, FTP- und SMTP- / POP3-Protokoll angezeigt. Diese Informationen können für den **letzten Tag** oder die **letzte Woche** angezeigt werden. Über entsprechende Links können Sie zwischen den einzelnen Ansichten navigieren.

Unter der Tabelle wird außerdem die Anzahl gefundener infizierter Objekte über den Zeitraum als Grafik dargestellt (gesplittet nach Stunden in der Ansicht für den letzten Tag und gesplittet nach Tagen in der Ansicht für die letzte Woche). Über das HTTP-Protokoll empfangene Objekte werden hierbei blau hervorgehoben. Über das FTP-Protokoll empfangene Objekte grün und über das SMTP- bzw. POP3-Protokoll empfangene Objekte rot.

BACKUP-ORDNER

Backup-Ordner: Ablageordner, in dem Originalkopien gefährlicher und passwortgeschützter Objekte vor der Verarbeitung gespeichert werden können. Objekte im Backup-Ordner können später auf dem Datenträger wiederhergestellt oder gelöscht werden. Diese Funktion kann nützlich sein, z.B.wenn während des Desinfektionsvorgangs Daten verloren gehen. Die Objekte im Backup-Ordner werden in einem speziellen Format gespeichert und stellen so keine Bedrohung für die Sicherheit der betreffenden Client-Computers dar.

Im Fenster (s. Abb. unten) wird eine Liste der im Backup-Ordner gespeicherten Objekte angezeigt. Für diese Objekte können Sie folgende Aktionen ausführen:

- Informationen zu den im Ordner gespeicherten Objekten anzeigen;
- Objekte auf Datenträgern speichern;
- Objekte löschen;
- Die Objektliste auf Datenträgern speichern.

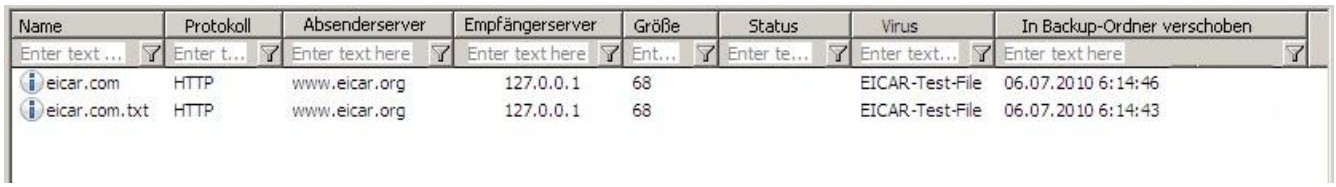

Abbildung 11. Fenster "Backup-Ordner"

Um Objekte leichter zu finden, können Sie folgende Arten von Filtern verwenden: dynamische (s. Abschnitt "Objektliste dynamisch filtern" ab S. 63) und statische (s. Abschnitt "Statischen Filter für Backup-Ordner erstellen" ab S. 64).

IN DIESEM ABSCHNITT

Funktionseinstellungen für den Backup-Ordner 62

Informationen zu Objekten im Backup-Ordner anzeigen 62

Ansicht des Backup-Ordners anpassen 63

Objektliste dynamisch filtern 63

Statischen Filter für Backup-Ordner erstellen 64

Objekte aus dem Backup-Ordner auf Datenträgern speichern 64

Objektliste des Backup-Ordners speichern 64

Objekte aus dem Backup-Ordner löschen 65

FUNKTIONSEINSTELLUNGEN FÜR DEN BACKUP-ORDNER

Um das Fenster zum Anpassen der Einstellungen für den Backup-Ordner aufzurufen, wählen Sie in der Konsolenstruktur den Knoten, für den gewünschten Server und anschließend den Knoten **Backup-Ordner**. Klicken Sie mit der rechten Maustaste auf das Kontextmenü im Ergebnisbereich rechts, und wählen Sie **Eigenschaften**.

Als Grundeinstellungen sind folgende Werte für die Einstellungen vorgegeben:

- **Maximale Speichergröße** – 1024 MB. Wird durch Hinzufügen eines neuen Objektes im Ordner dieser erlaubte Maximalwert überschritten, so werden die ältesten Objekte im Ordner gelöscht.
- **Maximale Aufbewahrungsfrist für Objekte** – 30 Tage. Nach Ablauf dieser Frist werden die betreffenden Objekte automatisch gelöscht.
- **maximale Anzahl Objekte im Ordner** – 1 Mio. Wird durch Hinzufügen eines neuen Objektes im Ordner diese erlaubte Maximalanzahl überschritten, so werden die ältesten Objekte im Ordner gelöscht.

Um erneut die Grundeinstellungen zu verwenden, klicken Sie auf die Schaltfläche **Standardwerte wiederherstellen**.

INFORMATIONEN ZU OBJEKTEN IM BACKUP-ORDNER ANZEIGEN

Um Informationen zu Objekten im Backup-Ordner anzuzeigen, gehen Sie folgendermaßen vor:

1. Wählen Sie in der Konsolenstruktur den Node für den gewünschten Server und anschließend den Node **Backup-Ordner**. Im Ergebnisbereich rechts wird das Fenster **Backup-Ordner** als Objektliste geöffnet.
2. Hier können Sie gewünschte Objekte suchen und deren Eigenschaften anzeigen. Bei Bedarf können Sie hierzu Filter verwenden (s. Abschnitt "Objektliste dynamisch filtern" ab S. 63).

Detailinformationen zu einzelnen Objekte können Sie über den Befehl **Eigenschaften** im Kontextmenü aufrufen. In dem folgenden Fenster werden Ihnen folgende Daten angezeigt:

- **Name**: Name der Datei.
- **Beschreibung**: Link zur Beschreibung des Objekts.
- **Virus**: Name des Virus.
- **Bericht**: Bericht, über welches das Objekt übertragen wurde.
- **Absenderserver**: Server, von dem die Datei versandt wurde.
- **Empfängerserver**: Server, auf dem die Datei empfangen wurde.
- **Status**: Status des Objekts
- **In Backup-Ordner verschoben**: Datum und Uhrzeit, zu dem das Objekt in den Backup-Ordner verschoben wurde.
- **Größe**: Größe des Objekts.
- **Erscheinungsdatum der Datenbanken**: Erscheinungsdatum und -uhrzeit der Datenbanken für Kaspersky Anti-Virus, mit deren Hilfe das Objekt gefunden wurde.

ANSICHT DES BACKUP-ORDNERS ANPASSEN

Sie können die Ansicht für den Backup-Ordner individuell anpassen, indem Sie einzelne Spalten der Tabelle hinzufügen oder löschen.

Um einzelne Spalten der Tabelle für den Backup-Ordner hinzuzufügen oder zu löschen, gehen Sie folgendermaßen vor:

1. Wählen Sie in der Konsolenstruktur den Node für den gewünschten Server und anschließend den Node **Backup-Ordner**. In der Ergebnisleiste rechts wird das Fenster **Backup-Ordner** geöffnet.

2. Wählen Sie im Kontextmenü des Fensters den Punkt **Ansicht** und anschließend **Spalten hinzufügen / Löschen**.

3. Verwenden Sie im folgenden Dialogfenster **Spalten hinzufügen / Löschen** die Schaltflächen **Hinzufügen** und **Löschen**, um verfügbare Spalten in die Spaltenliste zur Anzeige im Ergebnisbereich zu übernehmen oder zu entfernen.

4. Klicken Sie auf die Schaltfläche **OK**, um die vorgenommenen Änderungen zu speichern.

Die Spaltenbreite können Sie über die Tastenkombination **Ctrl+NumPlus** automatisch an die Breite des Spalteninhalts anpassen.

OBJEKTLISTE DYNAMISCH FILTERN

Die Verwendung dynamischer Filter erleichtert Ihnen die Suche und Strukturierung der Daten im Backup-Ordner, da bei Verwendung von Filtern nur die Daten angezeigt werden, die den gewählten Filtereinstellungen entsprechen. Mit dynamischen Filtern können Sie die Inhalte jeder beliebigen Spalte in der Tabelle filtern.

Um Objekte nach ausgewählten Kriterien mithilfe eines dynamischen Filters zu suchen, gehen Sie folgendermaßen vor:

1. Wählen Sie in der Konsolenstruktur den Knoten für den gewünschten Server und anschließend den Knoten **Backup-Ordner**. Im Ergebnisbereich rechts wird das Fenster **Backup-Ordner** als Objektliste geöffnet.

2. Im oberen Teil der Tabelle können Sie in den Eingabefeldern Filterkriterien für den dynamischen Filter festlegen. Legen Sie die Filterkriterien fest, indem Sie für jede Spalte die gewünschten Werte eingeben (Objekte können nach einer oder mehreren Spalten gefiltert werden).

3. Einige Sekunden nach Abschluss Ihrer Eingaben oder wenn Sie die Taste **ENTER** im Eingabefeld drücken, wird der Filter automatisch angewendet. Der Filter wird auch unmittelbar aktiviert, wenn Sie im Dropdown-Menü den entsprechenden Punkt auswählen oder auf die Schaltfläche **OK** im Eingabedialog klicken. Um den Filter anzuwenden, können Sie optional auch auf die Schaltfläche neben dem Eingabefeld für das Filterkriterium (wenn die Daten nur nach einem einzelnen Kriterium gefiltert werden sollen) bzw. auf die Schaltfläche **Aktualisieren** in der Werkzeugleiste von Kaspersky Anti-Virus klicken.

Über die Taste **F5** können Sie die Aktualisierung der Tabellenansicht für Objekte des Backup-Ordners erzwingen. So können Sie Informationen zu Objekten im Backup-Ordner stets in Echtzeit abrufen.

Um einen dynamischen Filter zu verwerfen und wieder alle Tabelleneinträge anzuzeigen, löschen Sie alle Zeichen aus den Eingabefeldern und starten Sie den Filter, oder wählen Sie im Dropdown-Menü für die entsprechenden Tabellenspalte den Punkt **Alle**.

STATISCHEN FILTER FÜR BACKUP-ORDNER ERSTELLEN

Um ausgewählte Filterkriterien mehrfach zu verwenden, können Sie im Knoten **Backup-Ordner** in der Konsolenstruktur der Management-Konsole statische Filter erstellen.

Um einen statischen Filter zu erstellen, gehen Sie folgendermaßen vor:

1. Markieren Sie in der Konsolenstruktur den Knoten für den **Backup-Ordner**.
2. Öffnen Sie das Kontextmenü, und wählen Sie den Punkt **Neuer Filter**. Der Assistent zum Erstellen eines neuen Filters wird geöffnet.
3. Folgen Sie den Anweisungen des Assistenten.

Um den neu erstellten Filter zu übernehmen, klicken Sie auf die Schaltfläche neben dem Feld für den Filter in der Tabelle, und wählen Sie im Kontextmenü der Schaltfläche den Punkt mit dem Namen des Filters.

OBJEKTE AUS DEM BACKUP-ORDNER AUF DATENTRÄGERN SPEICHERN

Um ein beliebiges Objekt aus dem Backup-Ordner auf Datenträgern zu speichern, gehen Sie folgendermaßen vor:

1. Markieren Sie in der Konsolenstruktur den Knoten **Backup-Ordner**.
2. Wählen Sie das Objekt für die Wiederherstellung in der Tabelle für den Inhalt des Backup-Ordners aus. Um Objekte zu suchen, können Sie Filter verwenden (s. Abschnitt "Objektliste dynamisch filtern" ab S. 63).
3. Öffnen Sie das Kontextmenü, und führen Sie den Befehl **Auf Datenträger speichern** bzw. den gleichlautenden Befehl im Menü **Aktion** aus.
4. Bestätigen Sie in der folgenden Warnmeldung das Wiederherstellen des Objekts mit Klick auf die Schaltfläche **Ja**.
5. Legen Sie in dem folgenden Fenster den Ordner fest, in dem das wiederhergestellte Objekt gespeichert werden soll, und ändern Sie bei Bedarf den Namen des Objekts oder geben Sie diesen neu ein.
6. Klicken Sie auf **Speichern**.

Das Objekt wird entschlüsselt und eine Kopie in dem von Ihnen bestimmten Ordner unter dem festgelegten Namen gespeichert. Das wiederhergestellte Objekt hat das gleiche Format, wie die Ursprungsdatei. Nachdem das Objekt erfolgreich gespeichert wurde, erhalten Sie eine entsprechende Bildschirmmeldung.

OBJEKTLISTE DES BACKUP-ORDNERS SPEICHERN

Die Objektliste für den Backup-Ordner können Sie als Textdatei speichern. Die Informationen zu den Objekten werden in Form einer Tabelle dargestellt.

Um die Objektliste für den Backup-Ordner als Textdatei zu speichern, gehen Sie folgendermaßen vor:

1. Wählen Sie in der Konsolenstruktur den Knoten für den gewünschten Server anschließend den Knoten **Backup-Ordner**.
2. Wählen Sie im Kontextmenü des Knotens **Backup-Ordner** den Punkt **Export List**.
3. Legen Sie im folgenden Dialogfenster den Ordner und die Datei fest, in welche die Objektliste exportiert werden soll.

4. Klicken Sie auf die Schaltfläche **Speichern**, um die Datei zu speichern.

OBJEKTE AUS DEM BACKUP-ORDNER LÖSCHEN

Folgende Objekte werden automatisch aus dem Backup-Ordner gelöscht:

- Die ältesten Objekte, wenn durch Hinzufügen neuer Objekte die zulässige Höchstzahl von 1 Mio. Objekten im Ordner überschritten wird.
- Die ältesten Objekte, falls durch Hinzufügen neuerer Objekte ein vorgegebener Maximalwert für die Größe des Backup-Ordners auf dem Datenträger überschritten wird.
- Objekte, deren Aufbewahrungsfrist abgelaufen ist, sofern eine maximale Aufbewahrungsdauer vorgegeben wurde.

Objekte aus dem Backup-Ordner können auch manuell gelöscht werden. Dies kann nützlich sein, wenn Sie z.B. erfolgreich wiederhergestellte Objekte löschen möchten, oder auch, um das Löschen von Objekten zu erzwingen, die durch automatische Löschvorgänge nicht erfasst wurden.

Um Objekte manuell aus dem Backup-Ordner löschen, gehen Sie folgendermaßen vor:

1. Wählen Sie in der Konsolenstruktur den Knoten **Backup-Ordner**.
2. Wählen Sie das Objekt zum Löschen in der Tabelle für den Inhalt des Backup-Ordners aus. Um Objekte zu suchen, können Sie Filter verwenden (s. Abschnitt "Objektliste dynamisch filtern" ab S. 63). Sie können auch mehrere oder alle Objekte gleichzeitig löschen. Markieren Sie hierzu alle Objekte, die Sie löschen möchten.
3. Öffnen Sie das Kontextmenü, und führen Sie den Befehl **Löschen** bzw. den gleichlautenden Befehl im Menü **Aktion** aus.
4. Bestätigen Sie das Löschen des Objekts im folgenden Dialogfenster

Anschließend werden die Objekte aus dem Backup-Ordner gelöscht.

DIAGNOSE

Sie können Kaspersky Anti-Virus so anpassen, dass Ereignisjournale geführt werden, um die Funktion des Programms zu jedem Zeitpunkt der Virenfilterung für Datenströme analysieren zu können.

Um das Fenster zum Anpassen der Diagnoseeinstellungen aufzurufen, gehen Sie folgendermaßen vor:

1. Wählen Sie in der Konsolenstruktur den Knoten für den gewünschten Server.
2. Klicken Sie auf die Schaltfläche **Allgemeine Parameter** in der Ergebnisleiste rechts.
3. Wechseln Sie zur Registerkarte **Diagnose** (s. Abb. unten).

Es werden folgende Journaltypen unterschieden:

- **Textjournale**: enthalten eine festgelegte Menge an Informationen zur Funktion des Programms zu einem bestimmten Datum. Format für den Dateinamen der Journaldatei: kavisaYYYYMMDD.log; hierbei ist DD – der aktuelle Tag, MM – der Monat, YYYY – das Jahr.
- **Textjournale**: enthalten eine festgelegte Menge an Informationen zur Funktion der Filter zu einem bestimmten Datum. Format für den Dateinamen der Journaldatei: kavfltYYYYMMDD.log; hierbei ist DD – der aktuelle Tag, MM – der Monat, YYYY – das Jahr.
- **Virenjournale**: enthalten Informationen über gefundene schädliche Objekte Filter zu einem bestimmten Datum. Format für den Dateinamen der Journaldatei: viruslogYYYYMMDD.log; hierbei ist DD – der aktuelle Tag, MM – der Monat, YYYY – das Jahr.

Die Journaldateien werden in einem separaten Ordner gespeichert, dessen Pfad Sie im Feld **Journalordner auf dem Server** finden können. Für geführte Journale können Sie folgende allgemeinen Einstellungen ändern:

- **Diagnosetiefe**. Für jedes Journal können Sie den Detaillierungsgrad vorgeben:
  - **Anderer**: Frei konfigurierbarer Detaillierungsgrad für Journale. Dieser ist nur für Textjournale verfügbar. Um den Eintrag anzupassen, klicken Sie auf die Schaltfläche Feineinstellung, und legen Sie den Detaillierungsgrad der Einträge für die einzelnen Programmkomponenten fest.
  - **Nicht ausgeben**: Keine Informationen Berichtieren.
  - **Minimal**: Nur die wichtigsten Ereignisse im Journal protokollieren. Dieser Wert ist auch in den Grundeinstellungen voreingestellt.
  - **Mittel**: Neben den wichtigsten eine Reihe weiterer Ereignisse zur Detailanalyse von Kaspersky Anti-Virus protokollieren.
  - **Maximal**: Größtmögliche Menge an Informationen im Journal protokollieren, mit Ausnahme von Testdaten.
  - **Testjournal**: Alle Informationen im Journal protokollieren, einschließlich Testdaten. Ist diese Diagnosetiefe gewählt, kann es sein, dass sehr viele Meldungen aufgezeichnet werden, wodurch die Performance des Computers beeinträchtigt und sehr schnell sehr viel Speicherplatz auf der Festplatte belegt wird. Deshalb sollten Sie diesen Modus lediglich für die Diagnose von Programmfehlern aktivieren.
- **Zeitpunkt von Ereignissen registrieren**. Zeitformat: **Universal Time Coordinated (UTC)** oder **lokale Zeit des Servers**. Als Standardwert ist **UTC** voreingestellt
- **Maximal N für jeden Journaltyp aufbewahren**. Anzahl der auf der Festplatte gespeicherten Journale. N kann Werte zwischen 1 und 365 annehmen. Der voreingestellte Standardwert beträgt - 5.

- **Neues Journal erstellen einmal in T**. T ist hierbei das Zeitintervall, mit dem neue Journale erstellt werden. Neue Dateien können einmal pro Tag, pro Woche oder pro Monat erstellt werden. Der voreingestellte Standardwert beträgt – Monat.

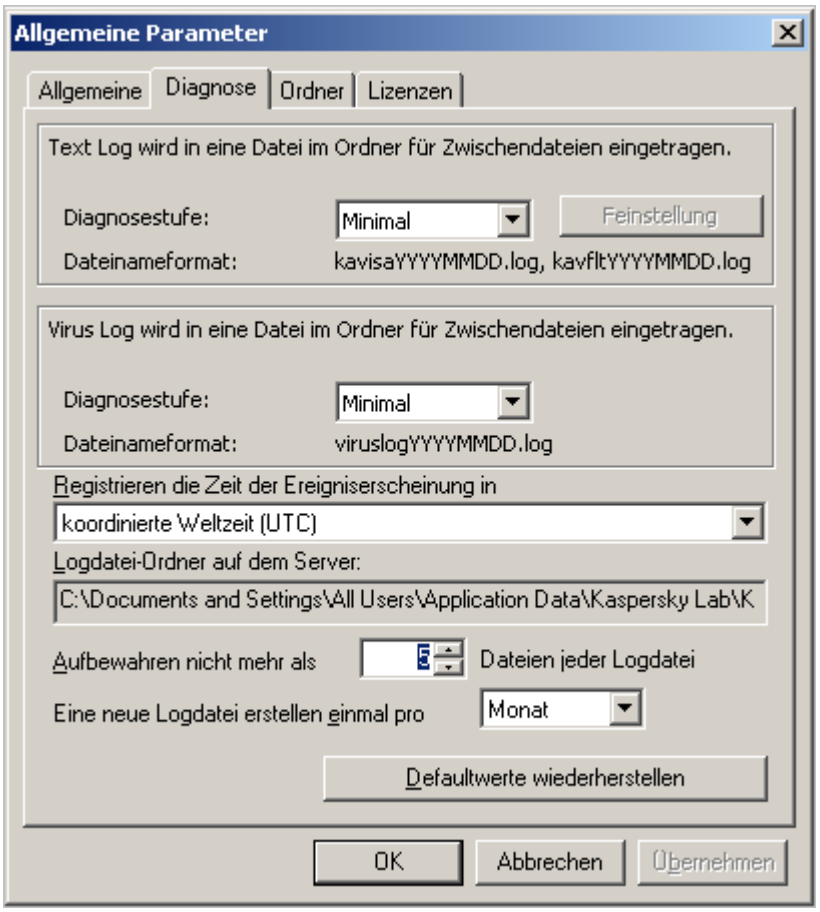

Abbildung 12. Registerkarte "Diagnose"

SPEICHERORT FÜR DEN DATENSPEICHERORDNER DES PROGRAMMS ÄNDERN

Um den Speicherort für den Datenspeicherordner des Programms und die darin enthaltenen Daten zu ändern, können Sie das Migrationstool **DataMigrationTool.exe** verwenden.

Um den Speicherort für die Programmdaten zu ändern, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Fenster der Microsoft-Windows-Konsole. Um dieses Fenster zu öffnen, haben Sie zwei Möglichkeiten:

   - Drücken Sie die Tastenkombination **WINDOWS KEY + R**;

   - Führen Sie in dem erscheinenden Dialogfenster **Ausführen** den Befehl `cmd` aus, und drücken Sie **ENTER**.

2. Machen Sie über den Befehl `cd [Pfad des Installationsordners von Kaspersky Anti-Virus]` den Installationsordner von Kaspersky Anti-Virus zum den Arbeitsordner der Microsoft-Windows-Konsole. z.B. `cd C:\Program Files\Kaspersky Lab\Kaspersky Anti-Virus 8.0 für Microsoft ISA Server und Forefront TMG Standard Edition\`. Den Pfad für den Installationsordner von Kaspersky Anti-Virus finden Sie im Fenster **Allgemeine Parameter** in der Registerkarte **Ordner** der Management-Konsole im Feld **Installationsordner des Programms**.

3. Führen Sie in der Microsoft-Windows-Konsole den Befehl `DataMigrationTool.exe [Pfad des neuen Datenspeicherordners] aus`. z.B. `DataMigrationTool.exe c:\data\KAV4ISA`. Falls der neue Datenspeicherordner für Kaspersky Anti-Virus bereits erstellt wurde, sollte er keine Daten enthalten.

4. Drücken Sie die **LEERTASTE**, um die Migration des Datenspeicherordners zu bestätigen.

5. Anschließend installiert das Tool die Dienste Microsoft Firewall und Kaspersky Anti-Virus, überprüft, ob alle Voraussetzungen für eine erfolgreiche Datenmigration erfüllt sind und beginnt mit dem Kopieren der Dateien. Nachdem die Dateien erfolgreich kopiert und die Änderungen in der Konfiguration registriert wurden, werden die gestoppten Dienste durch das Tool automatisch wieder gestartet.

6. Nachdem die Ausführung des Tools abgeschlossen ist, erhalten Sie folgende Bildschirmmeldung: Die Datenmigration in den Ordner [Pfad des neuen Datenspeicherordners] wurde erfolgreich abgeschlossen.

Den Pfad für den Datenspeicherordner von Kaspersky Anti-Virus finden Sie im Fenster **Allgemeine Parameter** in der Registerkarte **Ordner** der Management-Konsole im Feld **Datenspeicherordner des Programms**.

ÜBERWACHUNG FÜR DATENSTRÖME ÜBER DAS HTTPS-PROTOKOLL AKTIVIEREN

Für Forefront TMG wird auch der über das HTTPS-Protokoll eingehende Datenstrom überwacht. Für die Überwachung des Datenstroms über das HTTPS-Protokoll müssen Sie keine besonderen zusätzlichen Einstellungen vornehmen. Es werden die für das HTTP-Protokoll gewählten Einstellungen verwendet. Für die Überwachung des Datenstroms via HTTPS-Protokoll durch Kaspersky Anti-Virus müssen Sie die Überwachung des Datenstroms in der Management-Konsole von Forefront TMG aktivieren.

- *die Überwachung des Datenstroms via HTTPS-Protokoll zu aktivieren, gehen Sie folgendermaßen vor:*

1. Öffnen Sie die Management-Konsole von Forefront TMG.
2. Wählen Sie in der Konsolenstruktur der Management-Konsole den Knoten für den gewünschten Server und anschließend den Knoten **Web Access Policy**.
3. Klicken Sie in der Registerkarte **Tasks** Klicken Sie auf die Schaltfläche **Configure HTTPS Inspection**.
4. Markieren Sie im folgenden Fenster **HTTPS Outbound Inspection** in der Registerkarte **General** das Kästchen **Enable HTTPS Inspection**.
5. Klicken Sie auf die Schaltfläche **OK**, um das Fenster zu schließen.
6. Klicken Sie auf **Apply**, um die Änderungen zu speichern und die Konfiguration zu aktualisieren.

ANHANG 1. ÄNDERUNGEN IN DER MICROSOFT WINDOWS REGISTRY

Bei der Installation von Kaspersky Anti-Virus auf 32-Bit-Systemen werden in der Microsoft Windows Registry folgende Einträge geändert bzw. neu hinzugefügt:

HKEY_CLASSES_ROOT\AppID\{9F99C160-A3C7-438d-9BF8-76BE4D65370B}
HKEY_CLASSES_ROOT\AppID\{BE11C033-F253-400D-A7DC-931F193CDC9F}

HKEY_CLASSES_ROOT\AppID\kavisasrv.exe
HKEY_CLASSES_ROOT\AppID\KavHost.exe

HKEY_CLASSES_ROOT\CLSID\{162D6D1C-BEE9-4ae0-9E63-AA5E451A9985}
HKEY_CLASSES_ROOT\CLSID\{372C6E94-BA70-4493-893E-44A86EFA5FBA}
HKEY_CLASSES_ROOT\CLSID\{583F03A3-E02B-46D7-839D-4CBC63F82D59}
HKEY_CLASSES_ROOT\CLSID\{5CCFC1A2-A174-4A6C-9F84-B33C5FE14BF1}
HKEY_CLASSES_ROOT\CLSID\{620FF8BD-4798-4807-A2AB-F625B0EB3B44}
HKEY_CLASSES_ROOT\CLSID\{7A78B705-8CA4-4301-AADF-55F54E6A01AE}
HKEY_CLASSES_ROOT\CLSID\{84C221B0-73E9-4885-A044-30192B4DBC36}
HKEY_CLASSES_ROOT\CLSID\{92C67CDB-A762-43a7-A96D-E1A9D15686A5}
HKEY_CLASSES_ROOT\CLSID\{948600BB-5D4E-4808-B338-312257496A69}
HKEY_CLASSES_ROOT\CLSID\{9F3FD649-0012-4245-A443-CC23CFF9F713}
HKEY_CLASSES_ROOT\CLSID\{CFC47218-E213-405a-859E-2CEE0367ED6F}
HKEY_CLASSES_ROOT\CLSID\{D6E53EF2-B6B2-4A1A-ACF4-0F7B5C656D98}
HKEY_CLASSES_ROOT\CLSID\{D8CF93DF-788A-4699-9071-F3A854E5957C}
HKEY_CLASSES_ROOT\CLSID\{D8EE0CCE-F573-47cb-856B-37540B0DB34F}
HKEY_CLASSES_ROOT\CLSID\{DACDDD16-3454-49cc-B758-693FA413BB64}
HKEY_CLASSES_ROOT\CLSID\{E1F068E0-0FC0-4B8B-BE9A-6BDE3F496080}
HKEY_CLASSES_ROOT\CLSID\{F7CA6538-BCB6-44b0-A266-54C7C921F7C5}

HKEY_CLASSES_ROOT\Interface\{448D32AF-54D0-4BBD-8A81-C368E2C6E533}
HKEY_CLASSES_ROOT\Interface\{B620A5D5-8551-4887-B304-9800387A24CA}

HKEY_CLASSES_ROOT\KAV.ISD.IsaMmc.IsaAdmAbout
HKEY_CLASSES_ROOT\KAV.ISD.IsaMmc.IsaAdmAbout.1
HKEY_CLASSES_ROOT\KAV.ISD.IsaMmc.IsaAdmComponentData
HKEY_CLASSES_ROOT\KAV.ISD.IsaMmc.IsaAdmComponentData.1
HKEY_CLASSES_ROOT\KAV.ISD.ISAV.FtpFilter
HKEY_CLASSES_ROOT\KAV.ISD.ISAV.FtpFilter.1
HKEY_CLASSES_ROOT\KAV.ISD.ISAV.isavpop3.Pop3Filter
HKEY_CLASSES_ROOT\KAV.ISD.ISAV.isavpop3,Pop3Filter.1
HKEY_CLASSES_ROOT\KAV.ISD.ISAV.isavsmtp.SmtpFilter
HKEY_CLASSES_ROOT\KAV.ISD.ISAV.isavsmtp.SmtpFilter.1
HKEY_CLASSES_ROOT\KAV.ISD.ISAV.Watchdog3
HKEY_CLASSES_ROOT\KAV.ISD.ISAV.Watchdog3.1
HKEY_CLASSES_ROOT\KavHost.KavHost
HKEY_CLASSES_ROOT\KavHost.KavHost.1

HKEY_CLASSES_ROOT\TypeLib\{7FCD1648-8A7B-41AF-B76C-0699922B8770}

HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MMC\SnapIns\FX:{AA517B36-9B43-4246-9122-1AB672E4A6E1}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MMC\NodeTypes\{2F8FE3D1-9A16-4ED3-B6C6-F912D99E99FD}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MMC\SnapIns\{162D6D1C-BEE9-4ae0-9E63-AA5E451A9985}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MMC\SnapIns\{372C6E94-BA70-4493-893E-44A86EFA5FBA}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MMC\SnapIns\{620FF8BD-4798-4807-A2AB-F625B0EB3B44}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MMC\SnapIns\{92C67CDB-A762-43a7-A96D-E1A9D15686A5}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MMC\SnapIns\{948600BB-5D4E-4808-B338-312257496A69}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MMC\SnapIns\{CFC47218-E213-405a-859E-2CEE0367ED6F}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MMC\SnapIns\{D8CF93DF-788A-4699-9071-F3A854E5957C}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MMC\SnapIns\{D8EE0CCE-F573-47cb-856B-37540B0DB34F}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MMC\SnapIns\{F7CA6538-BCB6-44b0-A266-54C7C921F7C5}

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\SharedDlls
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{0D40E22B-2FB4-4237-AB63-3FFA9A4CE2EA}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Kaspersky Anti-Virus 8.0 for ISA Server and Forefront TMG SE
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Application\ISAV
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Application\KAV
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kavisasrv

Bei der Installation von Kaspersky Anti-Virus auf 64-Bit-Systemen werden in der Microsoft Windows Registry folgende Einträge geändert bzw. neu hinzugefügt:

HKEY_CLASSES_ROOT\AppID\{9F99C160-A3C7-438d-9BF8-76BE4D65370B}
HKEY_CLASSES_ROOT\AppID\{BE11C033-F253-400D-A7DC-931F193CDC9F}

HKEY_CLASSES_ROOT\AppID\kavisasrv.exe
HKEY_CLASSES_ROOT\AppID\KavHost.exe

HKEY_CLASSES_ROOT\CLSID\{583F03A3-E02B-46D7-839D-4CBC63F82D59}
HKEY_CLASSES_ROOT\CLSID\{5CCFC1A2-A174-4A6C-9F84-B33C5FE14BF1}
HKEY_CLASSES_ROOT\CLSID\{7A78B705-8CA4-4301-AADF-55F54E6A01AE}
HKEY_CLASSES_ROOT\CLSID\{7CBB6809-47B8-48D5-8ACD-8085935CCF6E}
HKEY_CLASSES_ROOT\CLSID\{84C221B0-73E9-4885-A044-30192B4DBC36}
HKEY_CLASSES_ROOT\CLSID\{9F3FD649-0012-4245-A443-CC23CFF9F713}
HKEY_CLASSES_ROOT\CLSID\{D6E53EF2-B6B2-4A1A-ACF4-0F7B5C656D98}

HKEY_CLASSES_ROOT\Interface\{448D32AF-54D0-4BBD-8A81-C368E2C6E533}
HKEY_CLASSES_ROOT\Interface\{B620A5D5-8551-4887-B304-9800387A24CA}
HKEY_CLASSES_ROOT\KAV.ISD.IsaMmc.IsaAdmAbout
HKEY_CLASSES_ROOT\KAV.ISD.IsaMmc.IsaAdmAbout.1
HKEY_CLASSES_ROOT\KAV.ISD.IsaMmc.IsaAdmComponentData
HKEY_CLASSES_ROOT\KAV.ISD.IsaMmc.IsaAdmComponentData.1
HKEY_CLASSES_ROOT\KAV.ISD.ISAV.FtpFilter
HKEY_CLASSES_ROOT\KAV.ISD.ISAV.FtpFilter.1
HKEY_CLASSES_ROOT\KAV.ISD.ISAV.isavpop3.Pop3Filter
HKEY_CLASSES_ROOT\KAV.ISD.ISAV.isavpop3,Pop3Filter.1
HKEY_CLASSES_ROOT\KAV.ISD.ISAV.isavsmtp.SmtpFilter
HKEY_CLASSES_ROOT\KAV.ISD.ISAV.isavsmtp.SmtpFilter.1
HKEY_CLASSES_ROOT\KAV.ISD.ISAV.Watchdog3
HKEY_CLASSES_ROOT\KAV.ISD.ISAV.Watchdog3.1
HKEY_CLASSES_ROOT\KavHost.KavHost
HKEY_CLASSES_ROOT\KavHost.KavHost.1

HKEY_CLASSES_ROOT\TypeLib\{7FCD1648-8A7B-41AF-B76C-0699922B8770}

HKEY_CLASSES_ROOT\Wow6432Node\AppID\{9F99C160-A3C7-438d-9BF8-76BE4D65370B}
HKEY_CLASSES_ROOT\Wow6432Node\AppID\{BE11C033-F253-400D-A7DC-931F193CDC9F}

HKEY_CLASSES_ROOT\Wow6432Node\AppID\KavHost.exe
HKEY_CLASSES_ROOT\Wow6432Node\AppID\kavisasrv.exe

HKEY_CLASSES_ROOT\Wow6432Node\CLSID\{162D6D1C-BEE9-4ae0-9E63-AA5E451A9985}
HKEY_CLASSES_ROOT\Wow6432Node\CLSID\{372C6E94-BA70-4493-893E-44A86EFA5FBA}
HKEY_CLASSES_ROOT\Wow6432Node\CLSID\{5CCFC1A2-A174-4A6C-9F84-B33C5FE14BF1}
HKEY_CLASSES_ROOT\Wow6432Node\CLSID\{620FF8BD-4798-4807-A2AB-F625B0EB3B44}
HKEY_CLASSES_ROOT\Wow6432Node\CLSID\{7A78B705-8CA4-4301-AADF-55F54E6A01AE}
HKEY_CLASSES_ROOT\Wow6432Node\CLSID\{7CBB6809-47B8-48D5-8ACD-8085935CCF6E}
HKEY_CLASSES_ROOT\Wow6432Node\CLSID\{92C67CDB-A762-43a7-A96D-E1A9D15686A5}
HKEY_CLASSES_ROOT\Wow6432Node\CLSID\{948600BB-5D4E-4808-B338-312257496A69}
HKEY_CLASSES_ROOT\Wow6432Node\CLSID\{9F3FD649-0012-4245-A443-CC23CFF9F713}
HKEY_CLASSES_ROOT\Wow6432Node\CLSID\{CFC47218-E213-405a-859E-2CEE0367ED6F}
HKEY_CLASSES_ROOT\Wow6432Node\CLSID\{D8CF93DF-788A-4699-9071-F3A854E5957C}
HKEY_CLASSES_ROOT\Wow6432Node\CLSID\{D8EE0CCE-F573-47cb-856B-37540B0DB34F}

HKEY_CLASSES_ROOT\Wow6432Node\CLSID\{DACDDD16-3454-49cc-B758-693FA413BB64}
HKEY_CLASSES_ROOT\Wow6432Node\CLSID\{E1F068E0-0FC0-4B8B-BE9A-6BDE3F496080}
HKEY_CLASSES_ROOT\Wow6432Node\CLSID\{F7CA6538-BCB6-44b0-A266-54C7C921F7C5}

HKEY_CLASSES_ROOT\Wow6432Node\Interface\{448D32AF-54D0-4BBD-8A81-C368E2C6E533}
HKEY_CLASSES_ROOT\Wow6432Node\Interface\{B620A5D5-8551-4887-B304-9800387A24CA}

HKEY_CLASSES_ROOT\Wow6432Node\KAV.ISD.IsaMmc.IsaAdmAbout
HKEY_CLASSES_ROOT\Wow6432Node\KAV.ISD.IsaMmc.IsaAdmAbout.1
HKEY_CLASSES_ROOT\Wow6432Node\KAV.ISD.IsaMmc.IsaAdmComponentData
HKEY_CLASSES_ROOT\Wow6432Node\KAV.ISD.IsaMmc.IsaAdmComponentData.1
HKEY_CLASSES_ROOT\Wow6432Node\KAV.ISD.ISAV.FtpFilter
HKEY_CLASSES_ROOT\Wow6432Node\KAV.ISD.ISAV.FtpFilter.1
HKEY_CLASSES_ROOT\Wow6432Node\KAV.ISD.ISAV.isavpop3,Pop3Filter
HKEY_CLASSES_ROOT\Wow6432Node\KAV.ISD.ISAV.isavpop3,Pop3Filter.1
HKEY_CLASSES_ROOT\Wow6432Node\KAV.ISD.ISAV.isavsmtp.SmtpFilter
HKEY_CLASSES_ROOT\Wow6432Node\KAV.ISD.ISAV.isavsmtp.SmtpFilter.1
HKEY_CLASSES_ROOT\Wow6432Node\KAV.ISD.ISAV.Watchdog3
HKEY_CLASSES_ROOT\Wow6432Node\KAV.ISD.ISAV.Watchdog3.1
HKEY_CLASSES_ROOT\Wow6432Node\KavHost.KavHost
HKEY_CLASSES_ROOT\Wow6432Node\KavHost.KavHost.1

HKEY_CLASSES_ROOT\Wow6432Node\TypeLib\{7FCD1648-8A7B-41AF-B76C-0699922B8770}

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\MMC\SnapIns\FX:{AA517B36-9B43-4246-9122-1AB672E4A6E1}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\MMC\NodeTypes\{2F8FE3D1-9A16-4ED3-B6C6-F912D99E99FD}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\MMC\SnapIns\{162D6D1C-BEE9-4ae0-9E63-AA5E451A9985}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\MMC\SnapIns\{372C6E94-BA70-4493-893E-44A86EFA5FBA}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\MMC\SnapIns\{620FF8BD-4798-4807-A2AB-F625B0EB3B44}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\MMC\SnapIns\{92C67CDB-A762-43a7-A96D-E1A9D15686A5}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\MMC\SnapIns\{948600BB-5D4E-4808-B338-312257496A69}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\MMC\SnapIns\{CFC47218-E213-405a-859E-2CEE0367ED6F}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\MMC\SnapIns\{D8CF93DF-788A-4699-9071-F3A854E5957C}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\MMC\SnapIns\{D8EE0CCE-F573-47cb-856B-37540B0DB34F}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\MMC\SnapIns\{F7CA6538-BCB6-44b0-A266-54C7C921F7C5}

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SharedDLLs
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{0D40E22B-2FB4-4237-AB63-3FFA9A4CE2EA}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Kaspersky Anti-Virus 8.0 for ISA Server and Forefront TMG SE
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Application\ISAV
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Application\KAV
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kavisasrv

INFORMATIONEN ZUM CODE VON DRITTHERSTELLERN

In diesem Abschnitt

Programmcode 73

Sonstige Informationen 78

Programmcode

Informationen zu verwendeten Quellcodes anderer Hersteller in Kaspersky Anti-Virus

In diesem Abschnitt

A C# IP ADDRESS CONTROL 73

BOOST 1.36.0, 1.39 74

EXPAT 1.2 74

LOKI 0.1.3 74

LZMALIB 4.43 75

MICROSOFT CABINET SOFTWARE DEVELOPMENT KIT 75

SQLITE 3.6.18 75

WIX 3.0 75

ZLIB 1.0.8, 1.2, 1.2.3 78

A C# IP ADDRESS CONTROL

Copyright (C) 2007, Michael Chapman

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE

FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

BOOST 1.36.0, 1.39.0

Copyright (C) 2008, Beman Dawes

Boost Software License - Version 1.0 - August 17th, 2003

Permission is hereby granted, free of charge, to any person or organization obtaining a copy of the software and accompanying documentation covered by this license (the "Software") to use, reproduce, display, distribute, execute, and transmit the Software, and to prepare derivative works of the Software, and to permit third-parties to whom the Software is furnished to do so, all subject to the following:

The copyright notices in the Software and this entire statement, including the above license grant, this restriction and the following disclaimer, must be included in all copies of the Software, in whole or in part, and all derivative works of the Software, unless such copies or derivative works are solely in the form of machine-executable object code generated by a source language processor.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

EXPAT 1.2

Copyright (C) 1998, 1999, 2000, Thai Open Source Software Center Ltd

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

LOKI 0.1.3

Copyright (C) 2001, by Andrei Alexandrescu

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE,

TITLE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

LZMALIB 4.43

MICROSOFT CABINET SOFTWARE DEVELOPMENT KIT

Copyright (C) 1993-1997, Microsoft Corporation

SQLITE 3.6.18

WIX 3.0

Copyright (C) Microsoft Corporation

Common Public License Version 1.0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS COMMON PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. DEFINITIONS

"Contribution" means:

a) in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and

b) in the case of each subsequent Contributor:

i) changes to the Program, and

ii) additions to the Program;

where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

"Contributor" means any person or entity that distributes the Program.

"Licensed Patents" mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

"Program" means the Contributions distributed in accordance with this Agreement.

"Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

2. GRANT OF RIGHTS

a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3. REQUIREMENTS

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a) it complies with the terms and conditions of this Agreement; and

b) its license agreement:

i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;

ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and

iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a) it must be made available under this Agreement; and

b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

4. COMMERCIAL DISTRIBUTION Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

5. NO WARRANTY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. DISCLAIMER OF LIABILITY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. GENERAL

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against a Contributor with respect to a patent applicable to software (including a cross-claim or counterclaim in a lawsuit), then any patent licenses granted by that Contributor to such Recipient under this Agreement shall terminate as of the date such litigation is filed. In addition, if Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. IBM is the initial Agreement Steward. IBM may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

ZLIB 1.0.8, 1.2, 1.2.3

Copyright (C) 1995-1998, Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly jloup@gzip.org

Mark Adler madler@alumni.caltech.edu

SONSTIGE INFORMATIONEN

Die Software kann einige Softwareprogramme enthalten, die an den Nutzer unter der GPL (GNU General Public License) oder sonstigen vergleichbaren freien Softwarelizenzen lizenziert (oder unterlizenziert) sind und dem Nutzer neben anderen Rechten gestatten, bestimmte Programme oder Teile dieser Programme zu kopieren, zu modifizieren und weiter zu verbreiten und sich Zugang zum Quellcode zu verschaffen ("Open Source Software"). Falls es solche Lizenzen erforderlich machen, dass für jedwede Software, die an jemanden in ausführbarem Binärformat geliefert wird, diesen Nutzern der Quellcode ebenfalls verfügbar gemacht wird, dann soll der Quellcode zur Verfügung gestellt werden, indem ein diesbezügliches Ersuchen an source@kaspersky.com gesendet wird, oder der Quellcode wird mit der Software geliefert.

Zur Überprüfung der elektronischen digitalen Signatur wird die Programmbibliothek für den Informationsschutz (PBSI) "Agava-C" eingesetzt, die von R-Alpha OOO entwickelt wurde.

ENDNUTZER-LIZENZVERTRAG FÜR KASPERSKY LAB SOFTWARE

WICHTIGER RECHTLICHER HINWEIS AN ALLE NUTZER: LESEN SIE FOLGENDE RECHTLICHE VEREINBARUNG SORGFÄLTIG DURCH, BEVOR SIE DIE SOFTWARE NUTZEN.

INDEM SIE IM LIZENZVERTRAG-FENSTER AUF DIE SCHALTFLÄCHE „AKZEPTIEREN" KLICKEN ODER EIN ENTSPRECHENDES ZEICHEN BZW. ENTSPRECHENDE ZEICHEN EINGEBEN, ERKLÄREN SIE SICH MIT DER EINHALTUNG DER GESCHÄFTSBEDINGUNGEN DIESES VERTRAGS EINVERSTANDEN. **DIESE AKTION KONSTITUIERT EIN BEKENNTNIS IHRER SIGNATUR UND SIE STIMMEN DIESER VEREINBARUNG, UND DASS SIE EINE PARTEI DIESER VEREINBARUNG WERDEN, ZU UND ERKLÄREN SICH WEITERHIN EINVERSTANDEN, DASS DIESE VEREINBARUNG, WIE JEDWEDE ANDERE SCHRIFTLICHE, AUSGEHANDELTE UND DURCH SIE UNTERZEICHNETE VEREINBARUNG AUCH, VOLLSTRECKBAR IST.** SOLLTEN SIE MIT DEN GESCHÄFTSBEDINGUNGEN DIESER VEREINBARUNG NICHT EINVERSTANDEN SEIN, BEENDEN SIE DIE INSTALLATION DER SOFTWARE BZW. INSTALLIEREN SIE SIE NICHT.

WENN DIE SOFTWARE MIT EINEM LIZENZVERTRAG ODER EINEM VERGLEICHBAREN DOKUMENT GELIEFERT WIRD, SIND DIE BEDINGUNGEN DER SOFTWARE-NUTZUNG GEMÄSS EINEM SOLCHEN DOKUMENT GEGENÜBER DIESEM ENDNUTZER-LIZENZVERTRAG MASSGEBEND.

NACHDEM SIE IM LIZENZVERTRAG-FENSTER AUF DIE SCHALTFLÄCHE „AKZEPTIEREN" GEKLICKT ODER EIN ENTSPRECHENDES ZEICHEN BZW. ENTSPRECHENDE ZEICHEN EINGEGEBEN HABEN, SIND SIE BERECHTIGT, DIE SOFTWARE IM EINKLANG MIT DEN GESCHÄFTSBEDINGUNGEN DIESER VEREINBARUNG ZU NUTZEN.

1. Definitionen

1.1. **Software** bezeichnet Software einschließlich aller Updates und zugehöriger Materialien.

1.2. **Rechtsinhaber** (Inhaber aller Rechte an der Software, ob exklusiv oder anderweitig) bezeichnet Kaspersky Lab ZAO, ein gemäß den Gesetzen der Russischen Föderation amtlich eingetragenes Unternehmen.

1.3. **Computer** bezeichnet/bezeichnen Hardware, einschließlich von PCs, Laptops, Workstations, PDAs, Smart Phones, tragbaren oder sonstigen elektronischen Geräten, für welche die Software konzipiert war und auf denen die Software installiert und/oder verwendet werden wird.

1.4. **Endnutzer (Sie)** bezeichnet eine bzw. mehrere Personen, die die Software in eigenem Namen installieren oder nutzen, oder die eine Software-Kopie rechtmäßig nutzt/nutzen, oder, falls die Software im Namen einer Organisation heruntergeladen oder installiert wurde, wie etwa einem Arbeitgeber, bezeichnet der Begriff *„Sie"* weiterhin jene Organisation, für die die Software heruntergeladen oder installiert wird, und es wird hiermit erklärt, dass eine solche Organisation die diese Vereinbarung akzeptierende Person autorisiert hat, dies in ihrem Namen zu tun. Im Sinne dieses Lizenzvertrags beinhaltet der Begriff *„Organisation"* ohne Einschränkungen jedwede Partnerschaft, GmbH, Gesellschaft, Vereinigung, Aktiengesellschaft, Treuhandgesellschaft, Gemeinschaftsunternehmen, Arbeitsorganisation, nicht eingetragene Organisation oder staatliche Behörde.

1.5. **Partner** bezeichnet Organisationen oder Personen, die die Software auf Grundlage eines Vertrags und einer mit dem Rechtsinhaber vereinbarten Lizenz vertreiben.

1.6. **Update(s)** bezeichnet/n alle Upgrades, Korrekturen, Patches, Erweiterungen, Reparaturen, Modifikationen, Kopien, Ergänzungen oder Wartungs-Softwarepakete usw.

1.7. **Benutzerhandbuch** bezeichnet die Bedienungsanleitung, die Administrator-Anleitung, ein Nachschlagewerk und ähnliche erläuternde oder sonstige Materialien.

2. Lizenzgewährung

2.1. Sie erhalten hiermit eine nicht-ausschließliche Lizenz zur Speicherung, zum Laden, zur Installation, Ausführung und Darstellung (zur „Nutzung") der Software auf einer festgelegten Anzahl von Computern zur Unterstützung des Schutzes Ihres Computers, auf dem die Software installiert ist, vor im Nutzerhandbuch beschriebenen Bedrohungen gemäß den technischen, im Benutzerhandbuch beschriebenen Anforderungen und im Einklang mit den Geschäftsbedingungen dieses Vertrags (die „Lizenz"). Sie erkennen diese Lizenz an.
Testversion. Sollten Sie eine Testversion der Software erhalten, heruntergeladen und/oder installiert haben und sollte Ihnen hiermit eine Evaluierungslizenz für die Software gewährt worden sein, dürfen Sie die Software ab dem Datum der ersten Installation nur zu Evaluierungszwecken verwenden, und zwar ausschließlich während der einzigen geltenden Evaluierungsperiode, außer wie anderweitig angegeben. Jegliche Nutzung der Software zu anderen Zwecken oder über die geltende Evaluierungsperiode hinaus ist strikt untersagt.

Software für mehrere Umgebungen; Mehrsprachige Software; Dual-Medien-Software; Mehrere Kopien; Softwarebündel. Wenn Sie verschiedene Versionen der Software oder verschiedene Sprachausgaben der Software verwenden, wenn Sie die Software auf mehreren Medien erhalten, wenn Sie anderweitig mehrere Kopien der Software erhalten oder wenn Sie die Software mit einer anderen Software gebündelt erhalten sollten, entspricht die insgesamt zulässige Anzahl Ihrer Computer, auf denen alle Versionen der Software installiert sind, der Anzahl der Computer, die in den Lizenzen festgelegt ist, die Sie bezogen haben, und jede erworbene Lizenz berechtigt Sie zur Installation und Nutzung der Software auf dieser Anzahl von Computern entsprechend den Festlegungen in den Klauseln 2.2 und 2.3, *außer die* Lizenzbedingungen sehen eine anderweitige Regelung vor.

2.2. Wenn die Software auf einem physischen Medium erworben wurde, haben Sie das Recht, die Software zum Schutz einer solchen Anzahl von Computern zu verwenden, die auf der Softwareverpackung festgelegt ist.

2.3. Wenn die Software über das Internet erworben wurde, haben Sie das Recht, die Software zum Schutz einer solchen Anzahl von Computern zu verwenden, die genannt wurde, als Sie die Lizenz für die Software erworben haben.

2.4. Sie haben das Recht, eine Kopie der Software anzufertigen, und zwar ausschließlich zu Sicherungszwecken und nur, um die rechtmäßig in Ihrem Besitz befindliche Kopie zu ersetzen, sollte eine solche Kopie verloren gehen, zerstört oder unbrauchbar werden. Diese Sicherungskopie kann nicht zu anderen Zwecken verwendet werden und muss zerstört werden, wenn Sie das Recht verlieren, die Software zu nutzen oder wenn Ihre Lizenz abläuft oder aus irgendeinem Grund im Einklang mit der gültigen Gesetzgebung im Land Ihres Wohnsitzes oder in dem Land, in dem Sie die Software nutzen, gekündigt werden sollte.

2.5. Ab dem Zeitpunkt der Aktivierung der Software bzw. Installation der Lizenzschlüsseldatei (mit Ausnahme einer Testversion der Software) haben Sie das Recht, folgende Dienstleistungen für den auf der Softwareverpackung (falls Sie Software auf einem physischen Medium erworben haben) oder während des Erwerbs (falls die Software über das Internet erworben wurde) festgelegten Zeitraum zu beziehen:

- Updates der Software über das Internet, wenn und wie der Rechtsinhaber diese auf seiner Webseite oder mittels anderer Online-Dienste veröffentlicht. Jedwede Updates, die Sie erhalten, werden Teil der Software und die Geschäftsbedingungen dieses Vertrags gelten für diese;
- Technische Unterstützung über das Internet sowie technische Unterstützung über die Telefon-Hotline.

3. Aktivierung und Zeitraum

3.1. Falls Sie Modifikationen an Ihrem Computer oder an der darauf installierten Software anderer Anbieter vornehmen, kann der Rechtsinhaber von Ihnen verlangen, die Aktivierung der Software bzw. die Installation der Lizenzschlüsseldatei zu wiederholen. Der Rechtsinhaber behält sich das Recht vor, jegliche Mittel und Verifizierungsverfahren zu nutzen, um die Gültigkeit der Lizenz und/oder die Rechtmäßigkeit einer Kopie der Software, die auf Ihrem Computer installiert und/oder genutzt wird, zu verifizieren.

3.2. Falls die Software auf einem physischen Medium erworben wurde, kann die Software nach Ihrer Annahme dieses Vertrags mit Beginn ab dem Zeitpunkt der Annahme dieses Vertrags für die auf der Verpackung bezeichnete Periode genutzt werden.

3.3. Falls die Software über das Internet erworben wurde, kann die Software nach Ihrer Annahme dieses Vertrags für die während des Erwerbs bezeichnete Zeitdauer genutzt werden.

3.4. Sie haben das Recht, eine Testversion der Software zu nutzen, und zwar gemäß der Festlegung in Klausel 2.1 und ohne jedwede Gebühr für die einzelne geltende Evaluierungsperiode (30 Tage) ab dem Zeitpunkt der Aktivierung der Software im Einklang mit diesem Vertrag, *und zwar unter der Bedingung, dass* die Testversion Ihnen nicht das Recht auf Updates und technische Unterstützung über das Internet und technische Unterstützung über die Telefon-Hotline einräumt.

3.5. Ihre Lizenz zur Nutzung der Software beschränkt sich auf den in den Klauseln 3.2 oder 3.3 (je nach Anwendbarkeit) bezeichneten Zeitraum. Die verbleibende Zeitdauer kann auf die im Benutzerhandbuch beschriebene Weise abgefragt werden.

3.6. Haben Sie die Software zur Nutzung auf mehr als einem Computer erworben, beginnt der Zeitraum, auf den Ihre Lizenz zur Nutzung der Software begrenzt ist, am Tag der Aktivierung der Software bzw. der Installation der Lizenzschlüsseldatei auf dem ersten Computer.

3.7. Unbeschadet anderer Rechtsmittel laut Gesetz oder Billigkeitsrecht, zu denen der Rechtsinhaber im Falle eines Verstoßes gegen die Geschäftsbedingungen dieses Vertrags durch Sie berechtigt ist, ist der Rechtsinhaber jederzeit, ohne Sie benachrichtigen zu müssen, dazu berechtigt, diese Lizenz zu kündigen, und zwar ohne den Verkaufspreis oder einen Teil davon zurückzuerstatten.

3.8. Sie stimmen zu, dass Sie bei der Nutzung der Software sowie bei der Verwendung jedweder Berichte oder Informationen, die sich als Ergebnis der Nutzung der Software ableiten, alle geltenden internationalen, nationalen, staatlichen, regionalen und lokalen Gesetze sowie gesetzlichen Bestimmungen, einschließlich (und ohne Beschränkung) Datenschutz-, Urheber-, Exportkontroll- und Verfassungsrecht, einhalten werden.

3.9. Außer wenn anderweitig hierin festgelegt, dürfen Sie keines der Rechte, die Ihnen unter diesem Vertrag gewährt werden, bzw. keine Ihrer hieraus entstehenden Pflichten übertragen oder abtreten.

4. Technische Unterstützung

4.1. Die in Klausel 2.5 dieses Vertrags erläuterte technische Unterstützung wird Ihnen gewährt, wenn das neueste Update der Software installiert wird (außer im Fall einer Testversion der Software).

Technischer Support: http://support.kaspersky.com

4.2. Die Daten des Benutzers, wie in Personal Cabinet/My Kaspersky Account festgelegt, können von den Experten vom Technischen Support nur während der Bearbeitung des Antrags des Benutzers verwendet werden.

5. Beschränkungen

5.1. Sie werden die Software nicht emulieren, klonen, vermieten, verleihen, leasen, verkaufen, modifizieren, dekompilieren oder zurückentwickeln oder disassemblieren oder Arbeiten auf Grundlage der Software oder eines Teils davon ableiten, jedoch mit der einzigen Ausnahme eines Ihnen durch geltende Gesetzgebung gewährten Rechts, von dem keine Rücktretung möglich ist, und Sie werden in keiner anderen Form irgendeinen Teil der Software in menschlich lesbare Form umwandeln oder die lizenzierte Software oder irgendeine Teilmenge der lizenzierten Software übertragen, noch irgendeiner Drittpartei gestatten, dies zu tun, außer im Umfang vorangegangener Einschränkungen, die ausdrücklich durch geltendes Recht untersagt sind. Weder Binärcode noch Quellcode der Software dürfen verwendet oder zurückentwickelt werden, um den Programmalgorithmus, der proprietär ist, wiederherzustellen. Alle Rechte, die nicht ausdrücklich hierin gewährt werden, verbleiben beim Rechtsinhaber und/oder dessen Zulieferern, je nachdem, was zutrifft. Jegliche derartige nicht autorisierte Nutzung der Software kann zur sofortigen und automatischen Kündigung dieses Vertrags sowie der hierunter gewährten Lizenz und zu Ihrer straf- und/oder zivilrechtlichen Verfolgung führen.

5.2. Sie werden die Rechte zur Nutzung der Software nicht an eine Drittpartei übertragen.

5.3. Sie werden den Aktivierungscode und/oder die Lizenzschlüssel-Datei keinen Drittparteien verfügbar machen oder Drittparteien Zugang zum Aktivierungscode und/oder zum Lizenzschlüssel gewähren. Aktivierungscode und/oder Lizenzschlüssel werden/wird als vertrauliche Daten des Rechtsinhabers betrachtet.

5.4. Sie werden die Software nicht an eine Drittpartei vermieten, verleasen oder verleihen.

5.5. Sie werden die Software nicht zur Erstellung von Daten oder Software verwenden, die zur Feststellung, zum Sperren oder zur Handhabung von Bedrohungen, wie im Nutzerhandbuch beschrieben, genutzt werden.

5.6. Ihre Schlüsseldatei kann blockiert werden, falls Sie gegen irgendwelche Geschäftsbedingungen dieses Vertrags verstoßen.

5.7. Falls Sie die Testversion der Software verwenden, sind Sie nicht berechtigt, technische Unterstützung, wie in Klausel 4 dieses Vertrags festgelegt, zu erhalten, und Sie sind ebenfalls nicht berechtigt, die Lizenz oder die Rechte zur Nutzung der Software an irgendeine Drittpartei zu übertragen.

6. Eingeschränkte Garantie und Haftungsausschluss

6.1. Der Rechtsinhaber garantiert, dass die Software im Wesentlichen im Einklang mit den im Nutzerhandbuch dargelegten Spezifikationen und Beschreibungen funktionieren wird, *jedoch vorausgesetzt,* dass eine solche eingeschränkte Garantie nicht für Folgendes gilt: (w) Mängel Ihres Computers und zugehörigen Verstoß, wofür der Rechtsinhaber ausdrücklich jedwede Gewährleistungsverantwortung ablehnt; (x) Funktionsstörungen, Defekte oder Ausfälle, resultierend aus falscher Verwendung, Missbrauch, Unfall, Nachlässigkeit, unsachgemäßer/m Installation, Betrieb oder Wartung, Diebstahl, Vandalismus, höherer Gewalt, terroristischen Akten, Stromausfällen oder -schwankungen, Unglück, Veränderung, nicht zulässiger Modifikation oder Reparaturen durch eine Partei außer dem Rechtsinhaber oder Maßnahmen einer sonstigen Drittpartei oder Aktionen ihrerseits, oder Ursachen außerhalb der Kontrolle des Rechtsinhabers; (y) jedweder Defekt, der dem Rechtsinhaber nicht durch Sie bekannt gemacht wird, sobald dies nach dem ersten Auftreten des Defekts möglich ist; und (z) Inkompatibilität, verursacht durch Hardware- und/oder Software-Komponenten, die auf Ihrem Computer installiert sind.

6.2. Sie bestätigen, akzeptieren und erkennen an, dass keine Software frei von Fehlern ist, und Sie sind angehalten, den Computer mit einer für Sie geeigneten Häufigkeit und Beständigkeit zu sichern.

6.3. Der Rechtsinhaber gibt keine Garantie, dass die Software im Fall von Verstößen gegen die Bedingungen, wie im Nutzerhandbuch oder in diesem Vertrag beschrieben, einwandfrei funktionieren wird.

6.4. Der Rechtsinhaber garantiert nicht, dass die Software einwandfrei funktionieren wird, wenn Sie nicht regelmäßig, wie in Klausel 2.5 dieses Vertrags erläutert, Updates herunterladen.

6.5. Der Rechtsinhaber garantiert keinen Schutz vor im Nutzerhandbuch beschriebenen Bedrohungen nach Ablauf der in Klausel 3.2 oder 3.3 dieses Vertrags bezeichneten Periode oder nachdem die Lizenz zur Nutzung der Software aus irgendeinem Grund gekündigt wurde.

6.6. DIE SOFTWARE WIRD OHNE MÄNGELGEWÄHR BEREITGESTELLT UND DER RECHTSINHABER GIBT KEINE ZUSICHERUNG UND KEINE GEWÄHRLEISTUNG IN BEZUG AUF IHRE NUTZUNG ODER LEISTUNG. DER RECHTSINHABER UND SEINE PARTNER GEWÄHREN AUßER DEN GARANTIEN, ZUSICHERUNGEN, BESTIMMUNGEN ODER BEDINGUNGEN, DIE DURCH GELTENDES RECHT NICHT AUSGESCHLOSSEN ODER BESCHRÄNKT WERDEN KÖNNEN, KEINE GARANTIEN, ZUSICHERUNGEN, BESTIMMUNGEN ODER BEDINGUNGEN (AUSDRÜCKLICHER ODER STILLSCHWEIGENDER NATUR, DIE ENTWEDER AUS EINER GESCHÄFTSBEZIEHUNG ODER EINEM HANDELSBRAUCH ENTSTEHEN BZW. AUS GESETZLICHEN, GEWOHNHEITSRECHTLICHTEN ODER ANDEREN VORSCHRIFTEN ABGELEITET WERDEN) HINSICHTLICH JEDWEDER ANGELEGENHEIT, EINSCHLIEßLICH (OHNE EINSCHRÄNKUNG) VON NICHTVERLETZUNG VON RECHTEN DRITTER, MARKTGÄNGIGKEIT, BEFRIEDIGENDE QUALITÄT, INTEGRIERUNG ODER BRAUCHBARKEIT FÜR EINEN BESTIMMTEN ZWECK. SIE TRAGEN DAS GESAMTE STÖRUNGSRISIKO UND DAS GESAMTRISIKO HINSICHTLICH DER LEISTUNG UND VERANTWORTUNG FÜR DIE AUSWAHL DER SOFTWARE, UM IHRE VORGESEHENEN RESULTATE ZU

ERZIELEN, UND FÜR DIE INSTALLATION SOWIE DIE NUTZUNG DER SOFTWARE UND DIE MIT IHR ERZIELTEN ERGEBNISSE. OHNE EINSCHRÄNKUNG DER VORANGEGANGENEN BESTIMMUNGEN MACHT DER RECHTSINHABER KEINE ZUSICHERUNGEN UND GIBT KEINE GEWÄHRLEISTUNG, DASS DIE SOFTWARE FEHLERFREI ODER FREI VON UNTERBRECHUNGEN ODER SONSTIGEN STÖRUNGEN IST ODER DASS DIE SOFTWARE JEDWEDE ODER ALL IHRE ANFORDERUNGEN ERFÜLLEN WIRD, UNGEACHTET DESSEN, OB GEGENÜBER DEM RECHTSINHABER OFFEN GELEGT ODER NICHT.

7. Haftungsausschluss und Haftungsbeschränkungen

7.1. INSOWEIT GESETZLICH STATTHAFT, SIND DER RECHTSINHABER UND SEINE PARTNER UNTER KEINEN UMSTÄNDEN HAFTBAR FÜR JEDWEDE SPEZIELLEN ODER BEILÄUFIGEN SCHÄDEN, STRAFZUSCHLAG ZUM SCHADENERSATZ, INDIREKTE ODER FOLGESCHÄDEN (EINSCHLIEßLICH UND NICHT BESCHRÄNKT AUF SCHÄDEN AUS VERLUST VON GEWINN ODER VERTRAULICHEN ODER SONSTIGEN INFORMATIONEN, FÜR GESCHÄFTSUNTERBRECHUNG, FÜR VERLUST VON PRIVATSPHÄRE, KORRUPTION, BESCHÄDIGUNG UND VERLUST VON DATEN ODER PROGRAMMEN, FÜR VERSÄUMNIS EINER PFLICHTERFÜLLUNG, EINSCHLIEßLICH JEDWEDER GESETZLICHER PFLICHTEN, TREUEPFLICHT ODER PFLICHT ZUR WAHRUNG ANGEMESSENER SORGFALT, FÜR NACHLÄSSIGKEIT, FÜR WIRTSCHAFTLICHEN VERLUST UND FÜR FINANZIELLEN ODER JEDWEDEN SONSTIGEN VERLUST), DIE AUS ODER AUF IRGENDEINE WEISE IM ZUSAMMENHANG MIT DER NUTZUNG ODER UNMÖGLICHKEIT DER NUTZUNG DER SOFTWARE, DER BEREITSTELLUNG ODER DEM VERSÄUMNIS DER BEREITSTELLUNG TECHNISCHER UNTERSTÜTZUNG ODER SONSTIGER DIENSTLEISTUNGEN, INFORMATIONEN, SOFTWARE UND ZUGEHÖRIGEM INHALT MITTELS DER SOFTWARE RESULTIEREN, ODER SICH ANDERWEITIG AUS DER NUTZUNG DER SOFTWARE ODER ANDERWEITIG UNTER BZW. IM ZUSAMMENHANG MIT EINER BESTIMMUNG DIESES VERTRAGS ERGEBEN, ODER DIE FOLGE EINES VERTRAGSBRUCHS ODER UNERLAUBTER HANDLUNG (EINSCHLIEßLICH NACHLÄSSIGKEIT, FALSCHANGABE, JEDWEDER STRIKTEN HAFTUNGSVERPFLICHTUNG ODER -PFLICHT), ODER EINER VERLETZUNG GESETZLICHER PFLICHTEN ODER DER GEWÄHRLEISTUNG DES RECHTSINHABERS UND/ODER EINES SEINER PARTNER SIND, UND ZWAR AUCH DANN NICHT, WENN DER RECHTSINHABER UND/ODER EINER SEINER PARTNER BEZÜGLICH DER MÖGLICHKEIT SOLCHER SCHÄDEN INFORMIERT WURDE.

SIE STIMMEN ZU, DASS IN DEM FALL, DASS DER RECHTSINHABER UND/ODER SEINE PARTNER HAFTBAR GEMACHT WERDEN/WIRD, DIE HAFTUNG DES RECHTSINHABERS UND/ODER SEINER PARTNER AUF DIE KOSTEN DER SOFTWARE BESCHRÄNKT IST. UNTER KEINEN UMSTÄNDEN WIRD DIE HAFTUNG DES RECHTSINHABERS UND/ODER SEINER PARTNER DIE FÜR DIE SOFTWARE ERSTATTETEN KOSTEN AN DEN RECHTSINHABER ODER DEN PARTNER ÜBERSTEIGEN (JE NACHDEM, WAS ZUTRIFFT).

NICHTS IN DIESEM VERTRAG SCHLIEßT EINEN ANSPRUCH AUFGRUND VON TOD UND PERSONENSCHADEN AUS ODER SCHRÄNKT DIESEN EIN. IN DEM FALL, DASS EIN HAFTUNGSAUSSCHLUSS, EIN AUSSCHLUSS ODER EINE EINSCHRÄNKUNG IN DIESEM VERTRAG AUFGRUND GELTENDEN RECHTS NICHT AUSGESCHLOSSEN ODER BESCHRÄNKT WERDEN KANN, WIRD NUR EIN SOLCHER HAFTUNGSAUSSCHLUSS, AUSSCHLUSS ODER EINE EINSCHRÄNKUNG NICHT FÜR SIE GELTEN, UND SIE SIND WEITERHIN AN JEDWEDE VERBLEIBENDEN HAFTUNGSAUSSCHLÜSSE, AUSSCHLÜSSE ODER EINSCHRÄNKUNGEN GEBUNDEN.

8. GNU und sonstige Drittpartei-Lizenzen

8.1. Die Software kann einige Softwareprogramme enthalten, die an den Nutzer unter der GPL (GNU General Public License) oder sonstigen vergleichbaren freien Softwarelizenzen lizenziert (oder unterlizenziert) sind und dem Nutzer neben anderen Rechten gestatten, bestimmte Programme oder Teile dieser Programme zu kopieren, zu modifizieren und weiter zu verbreiten und sich Zugang zum Quellcode zu verschaffen („Open Source Software"). Falls es solche Lizenzen erforderlich machen, dass für jedwede Software, die an jemanden in ausführbarem Binärformat geliefert wird, diesen Nutzern der Quellcode ebenfalls verfügbar gemacht wird, dann soll der Quellcode zur Verfügung gestellt werden, indem ein diesbezügliches Ersuchen an source@kaspersky.com gesendet wird, oder der Quellcode wird mit der Software geliefert. Falls irgendwelche Open Source Software-Lizenzen es erforderlich machen, dass der Rechtsinhaber Rechte zur Nutzung, zum Kopieren oder zur Änderung eines Open Source Software-Programms bereitstellt, welche umfassender sind, als die in diesem Vertrag gewährten Rechte, dann werden derartige Rechte Vorrang vor den hierin festgelegten Rechten und Einschränkungen haben.

9. Geistiges Eigentum

9.1. Sie stimmen zu, dass die Software sowie die Urheberschaft, Systeme, Ideen, Betriebsmethoden, Dokumentation und sonstige in der Software enthaltenen Informationen proprietäres geistiges Eigentum und/oder die wertvollen Geschäftsgeheimnisse des Rechtsinhabers oder seiner Partner sind und dass der Rechtsinhaber und seine Partner, je nachdem was zutrifft, durch das Zivil- und Strafrecht sowie durch Gesetze

zum Urheberrecht, bezüglich Geschäftsgeheimnissen, Handelsmarken und Patenten der Russischen Föderation, der Europäischen Union und der Vereinigten Staaten sowie anderer Länder und internationaler Übereinkommen geschützt sind. Dieser Vertrag gewährt Ihnen keinerlei Rechte am geistigen Eigentum, einschließlich an jeglichen Handelsmarken und Servicemarken des Rechtsinhabers und/oder seiner Partner („Handelsmarken"). Sie dürfen die Handelsmarken nur so weit nutzen, um von der Software im Einklang mit der akzeptierten Handelsmarkenpraxis erstellte Druckausgaben zu identifizieren, einschließlich der Identifizierung des Namens des Besitzers der Handelsmarke. Eine solche Nutzung der Handelsmarke gibt Ihnen keinerlei Besitzrechte an dieser Handelsmarke. Der Rechtsinhaber und/oder seine Partner besitzen und behalten alle Rechte, Titel und Anteile an der Software, einschließlich (ohne jedwede Einschränkung) jedweden Fehlerkorrekturen, Erweiterungen, Updates oder sonstigen Modifikationen an der Software, ob durch den Rechtsinhaber oder eine beliebige Drittpartei vorgenommen, und allen Urheberrechten, Patenten, Rechten an Geschäftsgeheimnissen, Handelsmarken und sonstigem geistigen Eigentum daran. Ihr Besitz, die Installation oder Nutzung der Software lässt den Titel am geistigen Eigentum an der Software nicht auf Sie übergehen, und Sie erwerben keinerlei Rechte an der Software, außer jene ausdrücklich in diesem Vertrag dargelegten. Alle hierunter erstellten Kopien der Software müssen dieselben proprietären Informationen enthalten, die auf und in der Software erscheinen. Mit Ausnahme der hierin aufgeführten Bestimmungen gewährt Ihnen dieser Vertrag keine Rechte geistigen Eigentums an der Software und Sie bestätigen, dass diese unter diesem Vertrag gewährte Lizenz Ihnen gemäß den weiteren Festlegungen hierin ausschließlich das Recht auf eingeschränkte Nutzung unter den Geschäftsbedingungen dieses Vertrags gewährt. Der Rechtsinhaber behält sich alle Rechte vor, die Ihnen nicht ausdrücklich in diesem Vertrag gewährt wurden.

9.2. Sie stimmen zu, die Software in keinster Weise zu modifizieren oder abzuändern. Sie dürfen die Urheberrechtshinweise oder sonstige proprietäre Hinweise auf jedweden Kopien der Software nicht entfernen oder verändern.

10. Geltendes Recht; Schiedsverfahren

10.1. Dieser Vertrag unterliegt den Gesetzen der Russischen Föderation und wird nach diesen ausgelegt, und zwar ohne Bezug auf gegenteilige gesetzliche Regelungen und Prinzipien. Dieser Vertrag wird nicht dem Übereinkommen der Vereinten Nationen über Verträge über den internationalen Warenverkauf unterliegen, dessen Anwendung ausschließlich ausgeschlossen wird. Jede Meinungsverschiedenheit, die aus den Bedingungen dieses Vertrags, deren Auslegung oder Anwendung oder einem Verstoß gegen diese resultiert, wird, außer falls durch unmittelbare Verhandlung beigelegt, durch das Gericht der internationalen Handelsschiedsgerichtsbarkeit bei der Industrie- und Handelskammer der Russischen Föderation in Moskau, in der Russischen Föderation, beigelegt. Jeder vom Schlichter abgegebene Schiedsspruch ist für die beteiligten Parteien endgültig und bindend und jedwedes Urteil bezüglich eines solchen Schiedsspruchs kann von jedem Gericht der zuständigen Jurisdiktion durchgesetzt werden. Nichts in diesem Abschnitt 10 wird eine Partei daran hindern, von einem Gericht der zuständigen Jurisdiktion rechtmäßige Entschädigung zu verlangen oder zu erhalten, sei es vor, während oder nach einem Schiedsverfahren.

11. Zeitraum für Rechtsverfolgung.

11.1. Von den Parteien dieses Vertrags kann keine Rechtsverfolgung, ungeachtet der Form, die sich aus Transaktionen unter diesem Vertrag ergibt, nach mehr als einem (1) Jahr nach dem Eintreten des Klagegrundes oder der Entdeckung dessen Eintritts ergriffen werden, außer, dass eine Rechtsverfolgung für Verletzung von Rechten geistigen Eigentums innerhalb des maximal geltenden gesetzlichen Zeitraums ergriffen wird.

12. Vollständigkeit der Vereinbarung, Salvatorische Klausel, kein Verzicht.

12.1. Dieser Vertrag stellt die Gesamtvereinbarung zwischen Ihnen und dem Rechtsinhaber dar und ersetzt jegliche sonstigen, vorherigen Vereinbarungen, Vorschläge, Kommunikation oder Ankündigung, ob mündlich oder schriftlich, in Bezug auf die Software oder den Gegenstand dieser Vereinbarung. Sie bestätigen, dass Sie diesen Vertrag gelesen haben, ihn verstehen und seinen Bedingungen zustimmen. Falls eine Bestimmung dieses Vertrags von einem Gericht der zuständigen Jurisdiktion insgesamt oder in Teilen als untauglich, ungültig oder aus welchen Gründen auch immer als nicht durchsetzbar angesehen wird, wird diese Bestimmung enger ausgelegt, damit sie rechtmäßig und durchsetzbar wird, und der Gesamtvertrag wird an diesem Umstand nicht scheitern, und die Ausgewogenheit des Vertrags bleibt weiterhin vollinhaltlich gültig und wirksam, so weit gesetzlich oder nach Billigkeitsrecht zulässig, während der ursprüngliche Inhalt weitest möglich beibehalten wird. Kein Verzicht auf eine hierin enthaltene Bestimmung oder Kondition ist gültig, außer in schriftlicher Form und durch Sie und einen autorisierten Vertreter des Rechtsinhabers unterzeichnet, vorausgesetzt, dass kein Verzicht einer Verletzung einer Bestimmung dieses Vertrags einen Verzicht eines vorherigen, gleichzeitigen oder Folgeverstoßes konstituiert. Nichtverfolgung oder fehlende Durchsetzung einer Bestimmung dieses Vertrags durch den Rechtsinhaber kann nicht als Verzicht auf diese Bestimmung oder dieses Recht geltend gemacht werden.

13. Kontaktinformationen des Rechtsinhabers.

Sollten Sie Fragen in Bezug auf diesen Vertrag haben oder sollten Sie wünschen, sich aus irgendeinem Grund mit dem Rechtsinhaber in Verbindung zu setzen, kontaktieren Sie bitte unsere Kundendienstabteilung unter:

Kaspersky Lab ZAO, 10 build. 1, 1st Volokolamsky Proezd
Moskau, 123060
Russische Föderation
Tel.: +7-495-797-8700
Fax: +7-495-645-7939
E-Mail: info@kaspersky.com
Webseite: www.kaspersky.com

© 1997-2010 Kaspersky Lab ZAO. Alle Rechte vorbehalten. Die Software und jedwede begleitende Dokumentation unterliegen dem Urheberrecht bzw. dem Schutz durch Urheberrechtsgesetze und internationale Urheberrechtsabkommen sowie durch weitere Gesetze und Abkommen zum geistigen Eigentum.

TERMINOLOGISCHES GLOSSAR

A

ADMINISTRATIONSGRUPPE

Die Administrationsgruppe ist eine Reihe von Computern, die entsprechend der auszuführenden Funktionen und der auf ihnen installierten Kaspersky-Lab-Anwendungen zusammengefasst werden. Die Gruppierung erfolgt zur einfachen Verwaltung der Computer als geschlossene Einheit. Zu einer Gruppe können andere Gruppen gehören. Für alle in der Gruppe installierten Anwendungen können Gruppenrichtlinien angelegt und Gruppenaufgaben erstellt werden.

AKTIVE LIZENZ

Das ist eine Lizenz, die aktuell für die Kaspersky-Lab-Anwendung verwendet wird. Sie bestimmt die Geltungsdauer für alle Programmfunktionen und die Lizenzrichtlinie für die Anwendung. In der Anwendung kann nie mehr als eine Lizenz den Status "aktiv" haben.

AUFGABE

Funktionen, die eine Kaspersky-Lab-Anwendung ausführt, zum Beispiel: Echtzeitschutz für Dateien, Vollständige Prüfung des Computers, Update der Datenbanken.

AUFGABEN FÜR ZUSAMMENSTELLUNG VON COMPUTERN

Die globale Aufgabe ist eine Aufgabe, die für eine Auswahl von Client-Computern auf beliebigen Administrationsgruppen des logischen Netzwerks festgelegt wurde und darauf ausgeführt werden soll.

AUFGABENEINSTELLUNGEN

Einstellungen für das Programm, die für jede Aufgabenart spezifisch sind

AUSNAHME

Eine Ausnahme ist ein Objekt, das von der Prüfung durch das Kaspersky-Lab-Programm ausgeschlossen wird. Von der Prüfung können Dateien eines bestimmten Formats, Dateien nach Maske, bestimmte Bereiche (beispielsweise ein Ordner oder Programm) sowie Programmprozesse oder Objekte nach einem Bedrohungstyp gemäß der Klassifikation der Viren-Enzyklopädie ausgeschlossen werden. Für jede Aufgabe können individuelle Ausnahmen festgelegt werden.

B

BERICHTS-TEMPLATE

Template zum Erstellen von Berichten zur Ausführung des Programms. In Berichts-Templates sind Einstellungen für den Berichtszeitraum, den Zeitplan für die Berichtserstellung und das Format von Berichten hinterlegt.

C

CONTAINER-OBJEKT

Objekt, das mehrere einzelne Bestandteile enthält, z.B. Archive und E-Mails mit beliebigen verschachtelten E-Mails). S. auch Einfaches Objekt.

D

DATEIMASKE

Platzhalter für den Namen und die Erweiterung einer Datei, der aus allgemeinen Zeichen besteht. Die zwei wichtigsten Zeichen, die in Dateimasken verwendet werden, sind * und ? (wobei * für eine beliebige Anzahl von Zeichen und ? für ein beliebiges Einzelzeichen steht). Mit Hilfe dieser Zeichen kann jede beliebige Datei dargestellt werden. Beachten Sie, dass Name und Endung einer Datei stets durch einen Punkt getrennt werden.

DATENBANKEN

Von Kaspersky Lab entwickelte Datenbanken mit genauen Definitionen aller aktuell bekannten Bedrohungen für Ihre Computersicherheit sowie den Algorithmen zum Auffinden und neutralisieren solcher Bedrohungen. Die Datenbanken werden von Kaspersky Lab laufend aktualisiert, sobald neue Bedrohungen bekannt werden.

DESINFEKTION VON OBJEKTEN

Methode zur Bearbeitung von infizierten Objekten, bei der die Daten vollständig oder teilweise wiederhergestellt werden oder eine Entscheidung darüber getroffen wird, dass die Desinfektion von Objekten nicht möglich ist. Die Desinfektion von Objekten erfolgt auf Basis der Einträge in den Datenbanken. Wenn die Desinfektion als primäre Aktion für ein Objekt gilt (erste Aktion mit dem Objekt, die sofort nach seinem Fund ausgeführt wird), wird eine Sicherungskopie des Objekts angelegt, bevor die Desinfektion ausgeführt wird. Bei der Desinfektion können Daten teilweise verloren gehen. Sie können diese Kopie verwenden, um ein Objekt in dem Zustand wiederherzustellen, wie vor der Desinfektion.

E

ERSATZ-TEMPLATE

Template für Informationsmeldungen, durch die der Textkörper von E-Mails ersetzt wird, wenn in der E-Mail oder in den Anhängen infizierte oder verdächtige Objekte gefunden wurden.

F

FIREWALL

Kombination von Hard- und/oder Softwarekomponenten zum Prüfen und Filtern durchlaufender Datenpakete im Netzwerk anhand vorgegebener Regeln. Hauptaufgabe der Firewall ist der Schutz von Computernetzen und einzelnen Netzwerkknoten vor unberechtigtem Zugriff. Für Firewalls wird synonym auch häufig der Begriff "Filter" verwendet, da da ihre wesentliche Funktion darin besteht, Datenpakete, die nicht den in der Konfiguration festgelegten Kriterien entsprechen, nicht passieren zu lassen (herauszufiltern).

G

GEFÄHRLICHES OBJEKT

Objekt, in dem sich ein Virus befindet. Es wird davor gewarnt, mit solchen Objekten zu arbeiten, weil dies zur Infektion des Computers führen kann. Beim Fund eines infizierten Objekts wird empfohlen, das Objekt mit Hilfe des Kaspersky-Lab-Programms zu desinfizieren oder, falls die Desinfektion nicht möglich ist, es zu löschen.

GRUPPENAUFGABE

Für eine Administrationsgruppe definierte Aufgabe, die auf allen Client-Computern dieser Administrationsgruppe ausgeführt wird.

GRUPPENRICHTLINIE

s. Richtlinie

H

HOST

Computer, auf dem Serversoftware läuft. Ein Host kann eine Vielzahl von Serverprogrammen ausführen, d.h. FTP-Server, Mailserver und Webserver können auf einem Host laufen. Ein Benutzer verwendet ein Client-Programm, beispielsweise einen Browser, um auf einen Host zuzugreifen. Häufig wird auch der Begriff Server verwendet, um einen Computer zu bezeichnen, auf dem Serversoftware läuft. Dadurch wird aber der praktische Unterschied zwischen Server und Host vernachlässigt.

Im Bereich der Telekommunikation ist der Host ein Computer, von dem Informationen eintreffen (wie z.B. FTP-Dateien, News oder Webseiten). Im Internet werden Hosts häufig als Knoten bezeichnet.

I

INFIZIERTES OBJEKT

Objekt, das schädlichen Code enthält: Bei der Prüfung des Objekts wurde erkannt, dass ein Abschnitt des Objektcodes vollständig mit dem Code einer bekannten Bedrohung übereinstimmt. Wir empfehlen Ihnen, solche Objekte nicht zu verwenden, da hierdurch Ihr Computer infiziert werden kann.

M

MANAGEMENT-KONSOLE

Die Management-Konsole ist eine Komponente von Kaspersky Administration Kit und bietet eine Benutzeroberfläche für die Administrationsdienste von Administrationsserver und Administrationsagenten.

MAXIMALE GESCHWINDIGKEIT

Wenn Sie diese Sicherheitsstufe wählen, werden nur die gefundenen potenziell infizierten Objekte überprüft. Dadurch wird die Ausführungszeit für die Virenprüfung wesentlich verkürzt.

MAXIMALER SCHUTZ

Sicherheitsstufe, die Ihrem Computer den maximalen Schutz bietet, den die Anwendung gewährleisten kann. Auf dieser Sicherheitsstufe werden alle Dateien des Computers sowie Wechseldatenträger und Netzlaufwerke auf Viren untersucht.

O

OBJEKT BLOCKIEREN

Der Zugriff externer Programme auf ein Objekt wird verboten. Ein blockiertes Objekt kann nicht gelesen, ausgeführt, verändert oder gelöscht werden.

P

PROGRAMM AKTIVIEREN

Freischalten aller Programmfunktionen. Für die Aktivierung des Programms benötigt der Benutzer eine Lizenz.

S

SCH

SCHLÜSSELDATEI

Die *.key-Datei, die Ihr persönlicher "Schlüssel" ist, wird zur Arbeit mit dem Programm Kaspersky Lab benutzt. Die Schlüsseldatei ist im Lieferumfang enthalten, wenn das Produkt beim Distributor von Kaspersky Lab gekauft wurde, oder Sie erhalten diese Datei per E-Mail, wenn das Produkt per Internet gekauft wurde.

SCHUTZ

Funktionsmodus des Programms, in dem Objekte im Echtzeitmodus auf schädlichen Code untersucht werden.

Das Programm fängt jeden Versuch zum Öffnen, Schreiben und Ausführen eines Objekts ab, und durchsucht das Objekt nach Bedrohungen. Virenfreie Objekte werden für den Zugriff freigegeben, infizierte oder verdächtige Objekte werden gemäß den Aufgabeneinstellungen verarbeitet (desinfiziert, gelöscht, in die Quarantäne verschoben).

SCHUTZSTATUS

Der aktuelle Zustand des Schutzes wird angezeigt, der das Sicherheitsniveau des Computers charakterisiert.

SCHWARZE LISTE FÜR SCHLÜSSELDATEIEN

Eine Datenbank, welche die Informationen über die von Kaspersky Lab blockierten Schlüsseldateien enthält. Der Inhalt der Datei mit der Blacklist wird zusammen mit den Datenbanken aktualisiert.

SPEICHER FÜR SICHERUNGSKOPIEN

Spezieller Ordner für die Speicherung von Kopien der Daten des Administrationsservers, die mit der Backup-Utility angelegt worden sind.

SUBNETZMASKE

Die Subnetzmaske (auch Netzwerkmaske genannt) und die Netzwerkadresse definieren die Adressen der Computer, die zu einem Netzwerk gehören.

U

UPDATE

Ein Vorgang zum Ersetzen / Hinzufügen neuer Dateien (Datenbanken und Programmodule), nach dem Herunterladen von den Kaspersky Lab Updateservern.

UPDATE DER DATENBANKEN

Eine Funktion, die vom Kaspersky-Lab-Programm ausgeführt wird und die es erlaubt, den aktuellen Zustand des Schutzes aufrecht zu erhalten. Dabei werden die Datenbanken von den Kaspersky-Lab-Updateservern auf den Computer kopiert und automatisch von der Anwendung übernommen.

V

VERFÜGBARES UPDATE

Paket von Updates für die Module der Kaspersky-Lab-Anwendung, zu dem dringende Updates zählen, die während eines bestimmten Zeitraums gesammelt wurden, und Änderungen an der Programmarchitektur.

VERTRAUENSWÜRDIGER PROZESS

Programmprozess, dessen Dateioperationen im Echtzeitschutz nicht von der Kaspersky-Lab-Anwendung kontrolliert werden. Das bedeutet, dass alle von einem vertrauenswürdigen Prozess gestarteten, geöffneten und gespeicherten Objekte nicht untersucht werden.

W

WIEDERHERSTELLUNG

Die Wiederherstellung ist ein Verschieben des ursprünglichen Objektes aus der Quarantäne oder aus dem Backup in den Ausgangsordner, in dem das Objekt bis zu dessen Verschieben in die Quarantäne, dessen Desinfektion oder Löschen gespeichert wurde, oder in einen anderen Ordner, den der Benutzer angegeben hat.

KASPERSKY LAB

Kaspersky Lab wurde 1997 gegründet. Heute sind wir das bekannteste Unternehmen für Datenschutz-Software in Russland und bieten eine breite Palette an Programmen zum Schutz vor Viren, unerwünschten E-Mails (Spam) und Hackerangriffen.

Kaspersky Lab ist eine internationale Gesellschaft. Unser Firmensitz befindet sich in Russland, regionale Vertretungen bestehen in Großbritannien, Frankreich, Deutschland, Japan, den Benelux-Staaten, China, Polen, Rumänien und den USA (Kalifornien). In Frankreich wurde jüngst ein neues Subunternehmen eröffnet - das Europäische Zentrum für Antivirenforschung. Unser Partnernetzwerk vereint weltweit mehr als 500 Firmen.

Bei Kaspersky Lab sind heutzutage mehr als tausend hochqualifizierte Spezialisten beschäftigt, zehn davon haben eine MBA-Ausbildung, sechzehn - Doktortitel. Führende Viren-Analytiker von Kaspersky Lab sind Mitglieder der angesehenen Organisation Computer Anti-Virus Researchers Organisation (CARO).

Das wertvollste Potenzial des Unternehmens sind einmaliges Know-how und Erfahrung, gesammelt durch unsere Mitarbeiter im Laufe von vierzehn Jahren ständigen Kampfes mit Computerviren. Durch die ständige Analyse der Entwicklung im Bereich Computerviren sind wir in der Lage, neue Tendenzen für gefährliche Programme vorherzusehen und den Anwendern frühzeitig zuverlässige Lösungen zum Schutz vor neuen Attacken anzubieten. Dies gilt als Grundlage für Produkte und Dienste von Kaspersky Lab. Wir sind unserer Konkurrenz stets einen Schritt voraus und garantieren maximale Sicherheit zum Wohle unserer Klientel.

In jahrelangen Bemühungen ist es uns gelungen, die Marktführerschaft in der Entwicklung von Virenschutzprogrammen zu erobern. Kaspersky Lab hat als erste Gesellschaft mehrere gegenwärtige Standarts für Anti-Viren-Programme ausgearbeitet. Die Basis-Software des Unternehmens heißt Kaspersky Anti-Virus und sie sorgt für einen zuverlässigen Schutz aller Objekte vor Virenangriffen: Arbeitsstationen, Dateiserver, Mail-Systeme, Firewalls und Internet-Gateways sowie Taschencomputer. Die bequeme Handhabung erlaubt einen größtenteils automatisierten Virenschutz in den Firmennetzwerken der Anwender. Viele Entwickler weltweit verwenden in ihrer Software den Kern vom Kaspersky Anti-Virus. Zu ihnen gehören u.a. Nokia ICG (USA), Aladdin (Israel), Sybari (USA), G Data (Deutschland), Deerfield (USA), Alt-N (USA), Microworld (Indien) und BorderWare (Kanada).

Den Kunden von Kaspersky Lab stehen zahlreiche Dienste zur Verfügung, die störungsfreien Betrieb der Produkte und exaktes Entsprechen der Geschäftsanforderungen garantieren. Wir planen, implementieren und warten Anti-Virenkomplexe für Unternehmen. Unsere Anti-Viren-Datenbanken werden alle drei Stunden aktualisiert. Unseren Anwendern bieten wir technische Unterstützung in mehreren Sprachen.

Bei Fragen wenden Sie sich an unsere Distributoren oder direkt an Kaspersky Lab (Kaspersky Lab ZAO). Wir werden Sie gern umfassend per Telefon oder E-Mail beraten. Weitere Information erhalten Sie bei:

Website von Kaspersky Lab:	http://www.kaspersky.com/de
Virenenzyklopädie:	http://www.securelist.com/de/
Anti-Virus-Labor:	newvirus@kaspersky.com (nur zum Einsenden verdächtiger Objekte in archivierter Form) http://support.kaspersky.ru/virlab/helpdesk.html?LANG=de (für Fragen an die Virenanalytiker)

SACHREGISTER

A

Aktionen mit Objekten 46
Anti-Viren-Kernel 39
Anwendungsbestimmung 7

B

BACKUP-ORDNER 61
Benutzerdefinierte Installation 15
Berichte
- anzeigen 55
- erstellen 55

BERICHTE 54

D

Datenbanken
- Anzahl Einträge 33
- automatisches Update 34
- Erstellungsdatum 33
- manuelles Update 34

Datenverkehr untersuchen 39, 40, 41, 42, 43
DIAGNOSETIEFE 66

E

EREIGNISJOURNAL 66

F

FUNKTIONSTEST 30

H

Hardwarevoraussetzungen 7

I

Installation
- Assistent 13
- benutzerdefinierte 15

Installation des Programms 13
Installationsmethode 15
Installationsordner 15

J

JOURNALORDNER 66

K

KASPERSKY LAB 89
Konsolenbaum 25

L

Lizenz
- Ersetzen 22
- reserve 23

Löschen
Aufgabe 56
Objekt 65
Richtlinie 50

M

Management-Konsole 25
MANAGEMENT-KONSOLE
STARTEN 28
Maximale Dauer der Objektuntersuchung 39
Maximale Größe
Quarantäne 62
zu untersuchendes Objekt 39
MMC 25

P

Programmhauptfenster 25
PROGRAMMOBERFLÄCHE 25
Programm-Update 13

Q

Quarantäne
die Anzeige der Objekte 62
löschen des Objekts 65

R

Richtlinien
erstellen 46
löschen 50
RICHTLINIEN 44

S

SERVER HINYUFÜGEN 29
Softwarevoraussetzungen 7
Speicherverzeichnisse
Backup-Ordner 61
STANDARDEINSTELLUNGEN 32
Starten
Update 34

U

Update
Nach Zeitplan 34
Startmodus 36
Updatequelle 35
Updatequelle 35

V

VERWALTUNG
LIZENZEN 22
Vollständige Installation 15